# Critical assessment of the extraterritoriality of the EU General Data Protection Regulation

University of Helsinki
Faculty of Law
Roman Beletski
Master's Thesis
Communication and information law
Supervisors: Päivi Korpisaari &
Susanna Lindroos-Hovinheimo
October 2019

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

| Tiedekunta – Fakultet – Faculty<br>Faculty of Law | | Koulutusohjelma – Utbildingsprogram – Degree Programme<br>Master of Laws |
|---|---|---|
| Tekijä – Författare – Author<br>Roman Beletski | | |
| Työn nimi – Arbetets titel – Title<br>Critical assessment of the extraterritoriality of the EU General Data Protection Regulation | | |
| Oppiaine/Opintosuunta – Läroämne/Studieinriktning – Subject/Study track<br>Communication and Information Law | | |
| Työn laji – Arbetets art – Level<br>Master's Thesis | Aika – Datum – Month and year<br>October 2019 | Sivumäärä – Sidoantal – Number of pages<br>xxviii + 87 |

Tiivistelmä – Referat – Abstract

It has long been the starting point in international law that a sovereign state is entitled to exclusively have control over the activity taking place on its soil, and that states should abstain from attempts to intervene in such internal affairs of each other. However, increasing globalisation and the advent of internet have shaken up this status quo – a traditional territorial approach to the regulation of novel phenomena in the online world is simply no longer sufficient. At the same time, overly broad extraterritorial claims by one state can be seen unacceptable by other states that are also interested in regulating the matter themselves. As it is discussed in this work, the contrast between these two approaches is highly relevant in the field of protection of personal data.

The aim of this work is to (1) examine the extent of the extraterritorial mechanisms of the EU General Data Protection Regulation, after which (2) a critical assessment of these mechanisms will be performed from the perspective of international law. Both of these questions will be reviewed from a mainly doctrinal point of view, with certain additional sociological arguments being presented in relation to question (1). When examining question (2), the doctrinal method will take on a critical dimension, as the assessment of reasonableness of the extraterritorial mechanisms of the GDPR will be performed using principles of public international law as a normative framework. In order to establish said framework, a review of the concepts of sovereignty, jurisdiction and extraterritoriality will take place in the beginning of the work. Due to the political nature of extraterritoriality, political viewpoints will also be considered, where relevant.

The GDPR employs several different mechanisms that stretch the Regulation's effects beyond the borders of the EU. Some of these effects are more direct than the others. First of all, the GDPR has a rather broad territorial scope under Article 3, pursuant to which the Regulation applies to non-EU controllers and processors that either have an establishment in the EU or target data subjects in the EU. In addition, the GDPR has an effect on controllers and processors receiving personal data from a data exporter in the EU, even if they would not be otherwise subject to the Regulation under its territorial scope. Furthermore, the European influence abroad is visible through the European Commission's adequacy decisions, bilaterally and multilaterally negotiated instruments, the Regulation's Brussels effect and even the public awareness concerning privacy matters that has been affected, at least indirectly, by the strict requirements of the EU data protection law.

In order to critically assess these mechanisms, a novel approach that accounts for all relevant factors when evaluating an extraterritorial assertion is assumed. While it is not possible to definitively claim that an extraterritorial claim is unacceptable, an overall assessment considering the principles of comity and sovereign equality can be helpful in order to establish whether certain extraterritorial assertions are questionable and to find alternative regulatory solutions that would be better in line with international law. Therefore, considering multiple factors, such as fairness, proportionality, justification, and predictability, it is concluded that certain extraterritorial mechanisms of the GDPR can be considered overly broad, especially when there is no real chance that they could be enforced. For this reason, the study suggests that special emphasis should be given to those extraterritorial mechanisms that are enforceable within the EU and to mechanisms that require no enforcement action in order to function. Additionally, a proper balance between the interests between the EU and other independent regulators needs to be sought when determining the extent of the requirements of the GDPR, as it was cautiously implied in the recent CJEU judgment in C-507/17 – *Google.*

Avainsanat – Nyckelord – Keywords
Data protection, extraterritoriality, extraterritorial effect, EU law, public international law, jurisdiction, sovereignty

Ohjaaja tai ohjaajat – Handledare – Supervisor or supervisors
Päivi Korpisaari and Susanna Lindroos-Hovinheimo

Säilytyspaikka – Förvaringställe – Where deposited
E-Thesis

Muita tietoja – Övriga uppgifter – Additional information

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

| | | |
|---|---|---|
| Tiedekunta – Fakultet – Faculty<br>Oikeustieteellinen tiedekunta | Koulutusohjelma – Utbildingsprogram – Degree Programme<br>Oikeustieteen maisteri | |
| Tekijä – Författare – Author<br>Roman Beletski | | |
| Työn nimi – Arbetets titel – Title<br>Critical assessment of the extraterritoriality of the EU General Data Protection Regulation | | |
| Oppiaine/Opintosuunta – Läroämne/Studieinriktning – Subject/Study track<br>Viestintä- ja informaatio-oikeus | | |
| Työn laji – Arbetets art – Level<br>Pro gradu -tutkielma | Aika – Datum – Month and year<br>Lokakuu 2019 | Sivumäärä – Sidoantal – Number of pages<br>xxviii + 87 |

Tiivistelmä – Referat – Abstract

Suvereenien valtioiden yksinoikeus säännellä omalla alueellaan tapahtuvaa toimintaa on toiminut vuosikymmenten ajan lähtökohtana kansainvälisessä oikeudessa. Tähän periaatteeseen sisältyy myös muiden valtioiden velvollisuus olla puuttumatta tällaisiin toisten valtioiden sisäisiin asioihin. Globalisaatio ja internetin kehitys ovat kuitenkin horjuttaneet tätä lähtökohtaa – territoriaalista lähestymistapaa ei voi enää pitää riittävänä takaamaan verkossa tapahtuvan toiminnan sääntelyn aukottomuutta ja tehokkuutta. Toisaalta, liian laajat ekstraterritoriaaliset vaatimukset voivat olla kyseenalaisia muiden valtioiden kannalta, sillä näillä valtioilla voivat olla omat intressit säännellä kyseistä toimintaa. Kuten tutkielmasta ilmenee, kyseinen lähestymistapojen vastakkainasettelu on erityisen relevantti henkilötietojen suojaa koskevan sääntelyn kontekstissa.

Tutkielman tavoitteina on (1) tarkastella EU:n yleisen tietosuoja-asetuksen (TSA) ekstraterritoriaalisia vaikutusmekanismeja ja näiden laajuutta, minkä jälkeen tarkoituksena on (2) arvioida näitä mekanismeja kriittisesti kansainvälisen oikeuden periaatteiden valossa. Tarkastelussa käytetään pääasiallisesti lainopillista metodia, minkä lisäksi kysymyksessä (1) esitetään tiettyjä sosiologisia lisäargumentteja. Kysymyksessä (2) lainopilliseen metodiin liittyy kriittinen näkökulma, koska TSA:n ekstraterritoriaalisten mekanismien kohtuullisuutta arvioidaan käyttämällä normatiivisena pohjana kansainvälisen julkisoikeuden periaatteita. Jotta tämä normatiivinen pohja voidaan perustaa, tutkielman alussa tutkitaan suvereniteetin, toimivallan (engl. j*urisdiction*) ja ekstraterritoriaalisuuden käsitteitä. Koska ekstraterritoriaalisuus on perusluonteeltaan poliittista, myös poliittisia näkökulmia otetaan esiin tarvittaessa.

TSA:ssa käytetään useita eri mekanismeja, joiden avulla asetuksen vaikutukset ulottuvat EU:n rajojen ulkopuolille. Osa näistä mekanismeista on suorempia kuin toiset. Ensinnäkin TSA:lla on 3 artiklan perusteella melko laaja alueellinen soveltamisala, minkä johdosta asetus soveltuu EU:n ulkopuolisiin rekisterinpitäjiin ja henkilötietojen käsittelijöihin, joilla joko on toimipiste EU:ssa tai jotka kohdistavat toimintansa unionissa sijaitseville rekisteröidyille. Lisäksi TSA vaikuttaa rekisterinpitäjiin ja käsittelijöihin, jotka vastaanottavat henkilötietoja tietojen viejältä EU:sta, vaikka kyseiset toimijat eivät muuten olisi asetuksen alaisia sen alueellisen soveltamisalan mukaisesti. Eurooppalaisen tietosuojalainsäädännön vaikutus ulkomailla näkyy myös Euroopan komission tietosuojan riittävyyttä koskevissa päätöksissä, kahden- ja monenkeskisesti neuvotelluissa asiakirjoissa, asetuksen Bryssel-efektissä ja jopa yleisessä yksityisyyskysymyksiä koskevassa valveutuneisuudessa, johon ovat vähintään epäsuorasti vaikuttaneet EU:n tietosuojalainsäädännön tiukat vaatimukset.

Näiden mekanismien kriittiseksi arvioimiseksi työssä käytetään uudenlaista lähestymistapaa, jossa huomioidaan kaikki ekstraterritoriaalisia väitteitä arvioidessa merkitykselliset tekijät. Vaikka ei olekaan mahdollista varmuudella väittää, ettei tiettyä ekstraterritoriaalista väitettä voi hyväksyä, kokonaisarviointi kansainvälisen kohteliaisuuden (engl. c*omity*) ja suvereenisen yhdenvertaisuuden periaatteiden valossa voi olla hyödyllinen. Tällainen kokonaisarvio on eduksi, kun tutkitaan ovatko tietyt ekstraterritoriaaliset väitteet kyseenalaisia ja selvitetään vaihtoehtoisia lainsäädännöllisiä ratkaisuja, jotka sopisivat paremmin kansainväliseen oikeuteen. Täten, ottaen huomioon useita eri tekijöitä, kuten reiluuden, suhteellisuuden, oikeutuksen ja ennakoitavuuden, päädytään siihen, että tiettyjä TSA:n ekstraterritoriaalisia mekanismeja voidaan pitää liian laajoina etenkin, kun niiden täytäntöönpanolle ei ole todellista mahdollisuutta. Tämän vuoksi tutkielmassa ehdotetaan, että erityistä painoarvoa tulisi antaa ensinnäkin niille ekstraterritoriaalisille mekanismeille, jotka ovat täytäntöönpantavissa EU:n sisällä ja toiseksi nille, jotka eivät edellytä lainkaan täytäntöönpanotoimenpiteitä toimiakseen. Lisäksi, kuten EUT varovasti viittasi viimeaikaisessa tuomiossaan asiassa C-507/17 – *Google*, on syytä etsiä asianmukaista tasapainoa EU:n ja muiden itsenäisten lainsäätäjien intressien välillä, kun määritellään TSA:n vaatimusten täytäntöönpanon laajuutta.

Avainsanat – Nyckelord – Keywords
Henkilötietojen suoja, tietosuoja, ekstraterritoriaalisuus, ekstraterritoriaalivaikutus, EU-oikeus, kansainvälinen julkisoikeus, toimivalta, suvereniteetti

Ohjaaja tai ohjaajat – Handledare – Supervisor or supervisors
Päivi Korpisaari ja Susanna Lindroos-Hovinheimo

Säilytyspaikka – Förvaringställe – Where deposited
E-Thesis

Muita tietoja – Övriga uppgifter – Additional information

# Contents

**Contents** ..... **iii**

**References** ..... **iv**
Literature ..... iv
Case law ..... xiv
Official documents ..... xviii
Online sources ..... xxiv

**Abbreviations** ..... **xxviii**

**1 Introduction** ..... **1**
1.1 Blurring the territorial borders ..... 1
1.2 The aims, the research questions and the scope of this thesis ..... 2
1.3 Methods ..... 5
1.4 Source material ..... 7

**2 Jurisdiction and extraterritoriality in international law** ..... **9**
2.1 Sovereignty ..... 9
2.2 Jurisdiction ..... 12
2.3 Extraterritoriality ..... 16
2.4 Issues related to extraterritoriality ..... 21
2.4.1 Justification of extraterritorial assertions ..... 22
2.4.2 Extraterritorial enforcement ..... 25
2.4.3 Potential limitations of extraterritoriality ..... 29

**3 Extraterritorial mechanisms of the GDPR** ..... **32**
3.1 General territorial scope of the GDPR (Article 3) ..... 33
3.1.1 Operator's establishment within the EU (Paragraph 1) ..... 33
3.1.2 Data subjects situated within the EU (Paragraph 2) ..... 38
3.1.3 GDPR applicable by virtue of public international law (Paragraph 3) ..... 45
3.2 Regulation of international data transfers (Articles 44–50) ..... 46
3.3 Effects caused by regulatory globalisation ..... 49
3.3.1 Regulatory globalisation through multilateral treaties and adequacy decisions ..... 49
3.3.2 Specific considerations concerning the EU–US relationship ..... 51
3.3.3 Unilateral regulatory globalisation (the Brussels Effect) ..... 55
3.4 Other effects ..... 58

**4 Assessment of the extraterritoriality of the GDPR** ..... **59**
4.1 Is the EU data protection regime extraterritorial? ..... 59
4.2 Are the extraterritorial claims justified? ..... 62
4.2.1 Justification under EU law ..... 62
4.2.2 Justification under international law ..... 63
4.3 Extraterritorial enforceability and enforcement of the EU data protection standards ..... 69
4.3.1 Enforceability in the case of non-compliance of a non-European operator ..... 69
4.3.2 Relationship between the territorial scope and regulation of international data transfers ..... 72
4.3.3 Extraterritorial implementation of data protection requirements ..... 74
4.4 A possible way forward? ..... 78
4.4.1 Gradual applicability of the data protection legislation ..... 78
4.4.2 Emphasis on "friendly" extraterritoriality ..... 81

**5 Concluding remarks** ..... **84**

# References

## Literature

Aarnio, Aulis: Oikeussäännön systematisointi ja tulkinta. Published in Häyhä, Juha (editor): Minun metodini. Werner Söderström lakitieto, 1997. *(Aarnio 1997)*

Akehurst, Michael: Jurisdiction in International Law. British Year Book of International Law, Vol. 46 (1972–1973), p. 145. *(Akehurst 1972–1973)*

Azzi, Adele: The Challenges Faced by the Extraterritorial Scope of the General Data Protection Regulation. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol. 9, Issue 2 (2018), p. 126. *(Azzi 2018)*

Bach, David – Newman, Abraham L.: The European regulatory state and global public policy: micro-institutions, macro-influence. Journal of European Public Policy, Vol. 14, No. 6 (2007), p. 827. *(Bach & Newman 2007)*

Bauchner, Joshua S.: State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate. Brooklyn Journal of International Law, Vol 26, No. 2 (2000), p. 689. *(Bauchner 2000)*

Berman, Franklin: Jurisdiction: The State. Published in Capps, Patrick – Evans, Malcolm – Konstantinidis, Stratos (editors): Asserting Jurisdiction: International and European Legal Approaches. Hart Publishing, 2003. *(Berman 2003)*

Bernhardt, Rudolf: Encyclopedia of Public International Law: Vol. 2, East African Community to Italy-United States Air Tansport Arbitration (1965). Elsevier, 1995. *(Bernhardt 1995)*

Bradford, Anu: The Brussels Effect. Northwestern University Law Review, Vol. 107, No. 1 (2012), p. 1. *(Bradford 2012)*

Brkan, Maja: Data Protection and Conflict-of-laws: A Challenging Relationship. European Data Protection Law Review (EDPL), Vol. 2, No. 3 (2016), p. 324. *(Brkan 2016)*

Brownlie, Ian: Principles of Public International Law. 7th ed. Oxford University Press, 2008. *(Brownlie 2008)*

Bu-Pasha, Shakila: Cross-border issues under EU data protection law with regards to personal data protection. Information & Communications Technology Law, Vol. 26, No. 3 (2017), p. 213. *(Bu-Pasha 2017)*

Buxbaum, Hannah L.: Territory, Territoriality, and the Resolution of Jurisdictional Conflict. American Journal of Comparative Law, Vol. 57, No. 3 (2009), p. 631. *(Buxbaum 2009)*

Bygrave, Lee Andrew: Determining Applicable Law Pursuant to European Data Protection Legislation. Computer Law and Security Report, Vol. 16 No. 4 (2000), p. 252. *(Bygrave 2000)*

Bygrave, Lee Andrew: Data Privacy Law: An International Perspective. Oxford University Press, 2014. *(Bygrave 2014)*

Capps, Patrick – Evans, Malcolm – Konstantinidis, Stratos (editors): Asserting Jurisdiction: International and European Legal Approaches. Hart Publishing, 2003. *(Capps et al. 2003)*

Cate, Fred H: The EU Data Protection Directive, Information Privacy, and the Public Interest. Iowa Law Review, Vol. 80, No. 3 (1995), p. 431*. (Cate 1995)*

Coughlan, Stephen – Currie, Robert – Kindred, Hugh – Scassa, Teresa: Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization. Canadian Journal of Law and Technology, Vol. 6, No. 1 (2007), p. 29*. (Coughlan et al. 2007)*

Crawford, James: Brownlie's Principles of Public International Law. 8th ed. Oxford University Press, 2012. *(Crawford 2012)*

Currie, John H: Public International Law. 2nd ed. Irwin Law 2008. *(Currie 2008)*

de Hert, Paul – Czerniawski, Michael: Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Vol. 6, No. 3 (2016), p. 230. *(de Hert & Czerniawski, 2016)*

de Lima Pinheiro, Luis: Law Applicable to Personal Data Protection on the Internet: Some Private International Law Issues. Anuario Espanol de Derecho Internacional Privado, Vol. 18 (2018), p. 161*. (de Lima Pinheiro 2018)*

Developments in the Law: Extraterritoriality. Harvard Law Review, Vol. 124, No. 5 (2011), p. 1226. *(Developments in the Law: Extraterritoriality 2011*)

Drezner, Daniel W: Globalization, harmonization, and competition: the different pathways to policy convergence. Journal of European Public Policy, Volume 12, No. 5 (2005), p. 841. *(Drezner 2005)*

Eichensehr, Kristen E.: Data Extraterritoriality, Texas Law Review – See Also, Vol. 95 (2016) p. 145. *(Eichensehr 2016)*

Emmenegger, Patrick – Eggenberger, Katrin: State sovereignty, economic interdependence and US extraterritoriality: the demise of Swiss banking secrecy and the re-embedding of international finance. Journal of International Relations and Development, Vol. 21, No. 3 (2018), p. 798. *(Emmenegger & Eggenberger 2018)*

Endicott, Timothy: The Logic of Freedom and Power. Published in Besson, Samantha – John Tasioulas: he Philosophy of International Law. Oxford University Press, 2010. *(Endicott 2010)*

Fox, James R: Dictionary of international and comparative law. 2nd ed. Oceana Publications, 1997. *(Fox 1997)*

Gady, Franz-Stefan: EU/U.S. Approaches to Data Privacy and the Brussels Effect: A Comparative Analysis. Georgetown Journal of International Affairs, Vol. 15, Special Issue (2014), p. 12. *(Gady 2014)*

Gerber, David J: The Extraterritorial Application of the German Antitrust Laws. American Journal of International Law, Vol. 77, No. 4 (1983), p. 756. *(Gerber 1983)*

Gerber, David J: Beyond Balancing: International Law Restraints on the Reach of National Laws. Yale Journal of International Law, Vol. 10, No. 1 (1984), p. 185. *(Gerber 1984)*

Goldsmith, Jack – Wu, Tim: Who controls the Internet? Illusions of a Borderless World. Oxford University Press, 2006. *(Goldsmith & Wu, 2006)*

Goldsmith, Jack: Unilateral Regulation of the Internet: A Modest Defence. European Journal of International Law, Vol. 11, No. 1 (2000), p. 135. *(Goldsmith 2000)*

Gömann, Merlin: The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement. Common Market Law Review, Vol. 54, No. 2 (2017), p. 567. *(Gömann 2017)*

Greenleaf, Graham: The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law Vol. 2, No. 2 (2012), p. 68. *(Greenleaf 2012)*

Greenleaf, Graham: Japan and Korea: Different paths to EU adequacy. Privacy Laws & Business International Report, Issue 156 (2018), p. 9. *(Greenleaf 2018)*

Greenleaf, Graham: It's Nearly 2020, so What Fate Awaits the 1980 OECD Privacy Guidelines? (A Background Paper for the 2019 OECD Privacy Guidelines Review). Privacy Laws & Business International Report, Issue 159 (2019), p. 18. *(Greenleaf 2019)*

Greze, Benjamin: The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives. International Data Privacy Law, Vol. 9, No. 2 (2019), p. 109. *(Greze 2019)*

Halpern, David: Inside the Nudge Unit: How small changes can make a big difference. WH Allen, 2015. *(Halpern 2015)*

Hart, H. L. A. – Bulloch, Penelope A. (editor) – Raz, Joseph (editor) – Green, Leslie (introduction): The concept of law. 3rd ed. Oxford University Press 2012. *(Hart 2012)*

Draft Convention on Jurisdiction with Respect to Crime. Supplement to the American Journal of International Law, Vol. 29 (1935), p. 435. *(Harvard Draft 1935)*

Hijmans, Hielke: European union as guardian of internet privacy: the story of Art 16 TFEU. Springer, 2016*. (Hijmans 2016)*

Hirvonen, Ari: Mitkä metodit? Opas Oikeustieteen Metodologiaan. Yleisen oikeustieteen julkaisuja 17, 2011*. (Hirvonen 2011)*

Hustinx, Peter: EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation. Collected Courses of the European University Institute's Academy of European Law, 24th Session on European Union Law, 1-12 July 2013. *(Hustinx 2013)*

Johnson, Gerry – Whittington, Richard – Scholes, Kevan – Angwin, Duncan – Regnér, Patrick: Exploring Strategy, Text and Cases. 11th edition. Pearson Education, 2017. *(Johnson et al. 2017)*

Kassan, Shalom: Extraterritorial Jurisdiction in the Ancient World. American Journal of International Law, Volume 29, No. 2 (1935), p. 237. *(Kassan 1935)*

Kelsen, Hans – Trevino, A. Javier (introduction): General Theory of Law and State. Transaction Publishers, 2005. *(Kelsen 2005)*

Kohl, Uta: Jurisdiction and the Internet: Regulatory Competence over Online Activity. Cambridge University Press. 2007. *(Kohl 2007)*

Kolehmainen, Antti: Tutkimusongelma ja metodi lainopillisessa työssä. Edilex, No. 29 (2015), p. 1. *(Kolehmainen 2015)*

Köndgen, Johannes: The Sources of European Private law. Published in Riesenhuber, Karl: European Legal Methodology. Intersentia, 2017. (Köndgen 2017)

Korpisaari, Päivi – Pitkänen, Olli – Warma, Eija: Uusi tietosuojalainsäädäntö. Alma Talent, 2018. *(Korpisaari et al. 2018)*

Koskenniemi, Martti: From apology to Utopia: the structure of international legal argument: reissue with a new epilogue. Cambridge University Press, 2005. *(Koskenniemi 2005)*

Kuner, Christopher: Data Protection Law and International Jurisdiction on the Internet (Part 1). International Journal of Law and Information Technology, Vol. 18, No. 2 (2010), p. 176. *(Kuner 2010a)*

Kuner, Christopher: Data Protection Law and International Jurisdiction on the Internet (Part 2). International Journal of Law and Information Technology, Vol. 18, No. 3 (2010), p. 227. *(Kuner 2010b)*

Kuner, Christopher: The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law, Bloomberg BNA Privacy and Security Law Report, 6 February (2012), p. 1. *(Kuner 2012)*

Kuner, Christopher: Transborder Data Flows and Data Privacy Law. Oxford University Press, 2013. *(Kuner 2013)*

Kuner, Christopher: The European Union and the Search for an International Data Protection Framework. Groningen Journal of International Law, Vol. 2, No. 2 (2014), p. 55. *(Kuner 2014)*

Kuner, Christopher: Extraterritoriality and regulation of international data transfers in EU data protection law. International Data Privacy Law, Vol. 5, No. 4 (2015), p. 235. *(Kuner 2015a)*

Kuner, Christopher: The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges. Published in Hess, Burkhard – Mariottini, Christina M. (editors): Protecting Privacy in Private International and Procedural Law and by Data Protection. Nomos, 2015. *(Kuner 2015b)*

Kuner, Christopher: Reality and Illusion in EU Data Transfer Regulation Post Schrems. German Law Journal, Vol. 18, No. 4 (2017), p. 881. *(Kuner 2017)*

Lam, Christina: Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner. Boston College International and Comparative Law Review, Vol. 40, E-Supplement (2017), p. 1*. (Lam 2017)*

Law, Stephanie: At the crossroads of consumer protection, data protection and private international law: some remarks on Verein fur Konsumenteninformation v Amazon EU. European Law Review, Vol. 42, No. 5 (2017), p. 751. *(Law 2017)*

Layton, Alexander – Parry, Angharad M.: Extraterritorial Jurisdiction – European Responses. Houston Journal of International Law, Vol. 26, No. 2 (2004), p. 309. *(Layton & Parry 2004)*

Lowe, A. V.: International Law. Oxford University Press, 2007. *(Lowe 2007)*

Lynskey, Orla: The Foundations of EU Data Protection Law. 1st edition. Oxford University Press, 2015. *(Lynskey 2015)*

Määttä, Tapio: Metodinen pluralismi oikeustieteessä – ympäristöoikeudellisen tutkimuksen suuntaukset ja menetelmät. Edilex, No 45 (2015), p. 1. *(Määttä 2015)*

Mann, F.A.: Studies in International Law. Clarendon Press, 1973. *(Mann 1973)*

McConville, Michael: Research Methods for Law. 2nd edition. Edinburgh University Press, 2017. *(McConville & Chui 2017)*

McCullagh, Karen: Cross-Border Data Protection: Applicable Law and Territorial powers of National Data Protection Supervisors. SCRIPTed: A Journal of Law, Technology and Society, Vol. 13, No. 1 (2016), p. 95. *(McCullagh 2016)*

Michaels, Ralf: Two Paradigms of Jurisdiction. Michigan Journal of International Law, Vol. 27, No. 4 (2006), p. 1003. *(Michaels 2006)*

Mills, Alex: The Confluence of Public and Private International Law: Justice, Pluralism and Subsidiarity in the International Constitutional Ordering of Private Law. Cambridge University Press, 2009. *(Mills 2009)*

Moerel, Lokke: The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? International Data Privacy Law, Vol. 1, No. 1 (2011), p. 28. *(Moerel 2011a)*

Moerel, Lokke: Back to basics: when does EU data protection law apply? International Data Privacy Law, Vol. 1, No. 2 (2011), p. 92. *(Moerel 2011b)*

Morrison, Andrew Stumpff: Law is the Command of the Sovereign: H.L.A. Hart Reconsidered. Ratio Juris, Vol. 29, No. 3 (2016), p. 364. *(Morrison 2016)*

Muse, Robert L: A Public International Law Critique of the Extraterritorial Jurisdiction of the Helms-Burton Act (Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996). George Washington Journal of International Law and Economics, Vol. 30, Nos. 2 and 3 (1996-1997), p. 207. *(Muse 1996-1997)*

Neergaard, Ulla B. – Nielsen, Ruth: Where Did the Spirit and Its Friends Go? On the European Legal Method(s) and the Interpretational Style of the Court of Justice of the European Union. Published in Neergaard, Ulla B. – Nielsen, Ruth – Roseberry, Lynn (editors): European legal method – paradoxes and revitalisation. DJØF, 2011. *(Neergaard & Nielsen 2011)*

Oppenheim, L. F. L. – Jennings, Robert (editor) – Watts, Arthur (editor): Oppenheim's International Law: Volume 1, Peace: Introduction and Part 1. 9th ed. Longman, 1996. *(Oppenheim et al. 1996)*

Perritt, Henry H: The Internet Is Changing the Public International Law System. Kentucky Law Journal, Vol. 88, No. 4 (2000), p. 885. *(Perritt 2000)*

Petkova, Bilyana: Domesticating the “foreign” in making transatlantic data privacy law. International Journal of Constitutional Law, Vol. 15, No. 4 (2018), p. 1135. *(Petkova 2018)*

Petkova, Bilyana: Privacy as Europe's first Amendment. European Law Journal, Vol. 25, No. 2 (2019), p. 140. *(Petkova 2019)*

Poullet, Yves: Transborder Data Flows and Extraterritoriality: the European Position. Journal of International Commercial Law and Technology, Vol. 2, No. 3 (2007), p. 141. *(Poullet 2007)*

Raitio, Juha: Euroopan unionin oikeus. Talentum Pro, 2016. *(Raitio 2016)*

Raustiala, Kal: Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law. Oxford University Press, 2009. *(Raustiala 2009)*

Reding, Viviane: The European data protection framework for the twenty-first century. International Data Privacy Law, Vol. 2, No. 3 (2012), p. 119. *(Reding 2012)*

Reed, Chris: Making laws for cyberspace. Oxford University Press, 2012. (Reed 2012)

Reichel, Jane: EU-rättslig metod. Published in: Nääv, Maria – Zamboni, Mauro: Juridisk metodlära. Andra upplagan. Lund: Studentlitteratur, 2018. *(Reichel 2018)*

Revolidis, Ioannis: Judicial Jurisdiction over Internet Privacy Violations and the GDPR: A Case of Privacy Tourism. Masaryk University Journal of Law and Technology, Vol. 11, No. 1 (Summer 2017), p. 7. *(Revolidis 2017)*

Riesenhuber, Karl: Interpretation of EU Secondary Law, Published in European Legal Methodology. Intersentia, 2017. *(Riesenhuber 2017)*

Ryngaert, Cedric: The concept of jurisdiction in international law. Published in Orakhelashvili, Alexander: Research Handbook on Jurisdiction and Immunities in International Law. Edward Elgar Publishing, 2015. *(Ryngaert 2015a)*

Ryngaert, Cedric: Jurisdiction in International Law. Second edition. Oxford University Press, 2015. *(Ryngaert 2015b)*

Schwartz, Paul M: The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. Harvard Law Review, Vol. 126, No. 7 (2013), p. 1966. *(Schwartz 2013)*

Scott, Joanne: The New EU Extraterritoriality. Common Market Law Review, Vol. 51, No. 5 (2014), p. 1343. *(Scott 2014a)*

Scott, Joanne: Extraterritoriality and Territorial Extension in EU Law. American Journal of Comparative Law, Vol. 62, No. 1 (2014), p. 87. *(Scott 2014b)*

Senz, Deborah – Charlesworth, Hilary: Australia's Response to Foreign Extraterritorial Legislation. Melbourne Journal of International Law, Vol. 2, No. 1 (2001), p. 69. *(Senz & Charlesworth 2001)*

Simitis, Spiros: Privacy – An Endless Debate? California Law Review, Vol. 98, No. 6 (2010), p. 1989. *(Simitis 2010)*

Sufrin, Brenda: Competition Law in a Globalised Marketplace: Beyond Jurisdiction. Published in Capps, Patrick – Evans, Malcolm – Konstantinidis, Stratos (editors): Asserting Jurisdiction: International and European Legal Approaches. Hart Publishing, 2003. *(Sufrin 2003)*

Svantesson, Dan Jerker B.: A "layered approach" to the extraterritoriality of data privacy laws. International Data Privacy Law, Vol. 3, No. 43 (2013), p. 278. *(Svantesson 2013a)*

Svantesson, Dan Jerker B.: Extraterritoriality in data privacy law. Ex Tuto Publishing, 2013. *(Svantesson 2013b)*

Svantesson, Dan Jerker B.: The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and its Practical Effect on U.S. Business. Stanford Journal of International Law, Vol. 50, No. 1 (2014), p. 53. *(Svantesson 2014)*

Svantesson, Dan Jerker B.: A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, AJIL Unbound, Vol. 109 (2015-2016), p. 69. *(Svantesson 2015-2016)*

Svantesson, Dan Jerker B.: Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation. International Data Privacy Law, Vol. 5, No. 4 (2015), p. 226. *(Svantesson 2015a)*

Svantesson, Dan Jerker B.: A Jurisprudential Justification for Extraterritoriality in (Private) International Law. Santa Clara Journal of International Law, Vol. 13, No. 2 (2015), p. 517. *(Svantesson 2015b)*

Svantesson, Dan Jerker B.: Article 4(1)(a) ‘establishment of the controller’ in EU data privacy law—time to rein in this expanding concept? International Data Privacy Law, Vol. 6, No. 3 (2016), p. 210. *(Svantesson 2016a)*

Svantesson, Dan Jerker B.: The CJEU’s Weltimmo Data Privacy Ruling – Lost in the Data Privacy Turmoil, Yet So Very Important. Maastricht Journal of European and Comparative Law, Vol. 23, No. 2 (2016), p. 332. *(Svantesson 2016b)*

Svantesson, Dan Jerker B.: Solving the Internet Jurisdiction Puzzle. 1st edition. Oxford University Press, 2017. *(Svantesson 2017)*

Svantesson, Dan Jerker B.: European Union Claims of Jurisdiction over the Internet. Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol. 9, No. 2 (2018), p. 113. *(Svantesson 2018)*

Talus, Kim – Penttinen, Sirja-Leena: Eurooppaoikeudelliset oikeuslähteet ja niiden tulkinta oikeustieteellistä opinnäytettä kirjoitettaessa. Edilex, No. 3 (2015), p. 1. *(Talus & Penttinen 2015)*

Taylor, Mistale: Google Spain Revisited. European Data Protection Law Review (EDPL), Vol. 3, No. 2 (2017), p. 195. *(Taylor 2017)*

Tene, Omer – Wolf, Christopher: Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation. The Future of Privacy Forum White Paper, January 2013. *(Tene & Wolf 2013)*

Tiilikainen, Teija – Helander, Petri – Heliskoski, Joni: Euroopan perustuslaki. Edita, 2005. *(Tiilikainen et al. 2005)*

Tuori, Kaarlo: Kriittinen oikeuspositivismi. Werner Söderström lakitieto, 2000. *(Tuori 2000)*

Van Alsenoy, Brendan – Koekkoek, Marieke: Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted'. International Data Privacy Law, Vol. 5, No. 2 (2015), p. 105. *(Van Alsenoy & Koekkoek 2015)*

Weber, Rolf H.: Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. International Data Privacy Law, 2013, Vol. 3, No. 2 (2013), p. 117. *(Weber 2013)*

Whitman, James Q: The Two Western Cultures of Privacy: Dignity versus Liberty. Yale Law Journal, Vol. 113, No. 6 (2004), p. 1151. *(Whitman 2004)*

Wimmer, Kurt: Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers? Syracuse Law Review, Vol. 68, No. 3 (2018), pp. 547. *(Wimmer 2018)*

Zhuravlev, Mikhail S. – Brazhnik, Tatiana A.: Russian data retention requirements: Obligation to store the content of communications. Computer Law and Security Review, Vol. 34, No. 3 (2018), p. 496. *(Zhuravlev & Brazhnik 2018)*

Zielonka, Jan: Europe as a Global Actor: Empire by Example? International Affairs, Vol. 84, No. 3 (2008), p. 471. *(Zielonka 2008)*

**Case law**

***International Court of Justice (Permanent Court of International Justice)***

The Case of the S.S. "Lotus", Publications of the Permanent Court of International Justice, Series A, No. 10, delivered on 7 September 1927. *(The Case of SS Lotus)*

Barcelona Traction, Light and Power Company, Limited, Judgment, I.C.J. Reports 1970, p. 3, delivered on 5 February 1970. *(Barcelona Traction, Light and Power Co, Ltd)*

***Permanent Court of Arbitration***

Island of Palmas case (United Nations Reports of International Arbitral Awards, Volume II, pp. 829-871), delivered on 4 April 1928. *(Island of Palmas Case)*

***Court of Justice of the European Union***

Case 26-62 – NV Algemene Transport- en Expeditie Onderneming van Gend & Loos v Netherlands Inland Revenue Administration, delivered on 5 February 1963. *(C-26/62 – Van Gend en Loos)*

Case 48-69 – Imperial Chemical Industries Ltd. v Commission of the European Communities, delivered on 14 July 1972. *(C-48/69 – ICI v Commission)*

Joined cases C-89/85, C-104/85, C-114/85, C-116/85, C-117/85 and C-125/85 to C-129/85 – A. Ahlström Osakeyhtiö and others v Commission of the European Communities, delivered on 27 September 1988. *(C-89/85 – Ahlström Osakeyhtiö and Others v Commission)*

Case T-102/96 – Gencor Ltd v Commission of the European Communities, delivered on 25 March 1999. *(T-102/96 – Gencor v Commission)*

Case C-101/01 – Criminal proceedings against Bodil Lindqvist, delivered on 6 November 2003. *(C-101/01 – Lindqvist)*

Joined cases C-402/05 P and C-415/05 P – Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities, delivered on 3 September 2008. *(C-402/05 P – Kadi and Al Barakaat International Foundation v Council and Commission)*

Joined cases C-585/08 and C-144/09 – Peter Pammer v Reederei Karl Schlüter GmbH & Co. KG and Hotel Alpenhof GesmbH v Oliver Heller, delivered on 7 December 2010. *(C-585/08 – Pammer and Hotel Alpenhof)*

Case C-366/10 – Air Transport Association of America and Others v Secretary of State for Energy and Climate Change, delivered on 21 December 2011. *(C-366/10 – Air Transport Association of America and Others)*

Case C-190/11 – Daniela Mühlleitner v Ahmad Yusufi and Wadat Yusufi, delivered on 6 September 2012. *(C-190/11 – Mühlleitner)*

Joined Cases C-584/10 P, C-593/10 P and C-595/10 P – European Commission and Others v Yassin Abdullah Kadi, delivered on 18 July 2013. *(C-584/10 P – Commission and Others v Kadi)*

Case C-218/12 – Lokman Emrek v Vlado Sabranovic, delivered on 17 October 2013. *(C-218/12 – Emrek)*

Case C-131/12 – Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, delivered on 13 May 2014. *(C-131/12 – Google Spain and Google)*

Case C-230/14 – Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, delivered on 1 October 2015. *(C-230/14 – Weltimmo)*

Case C-362/14 – Maximillian Schrems v Data Protection Commissioner, delivered on 6 October 2015. *(C-362/14 – Schrems)*

Case C-192/15 – T. D. Rease and P. Wullems v College bescherming persoonsgegevens, removed from register on 9 December 2015. *(C-192/15 – Rease and Wullems)*

Case C-191/15 – Verein für Konsumenteninformation v Amazon EU Sàrl, delivered on 28 July 2016. *(C-191/15 – Verein für Konsumenteninformation)*

Case C-413/14 P – Intel Corp. v European Commission, delivered on 6 September 2017. *(C-413/14 P – Intel v Commission)*

Case C-210/16 – Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, delivered on 5 June 2018. *(C-210/16 – Wirtschaftsakademie Schleswig-Holstein)*

Case C-496/17 – Deutsche Post AG v Hauptzollamt Köln, delivered on 16 January 2019. *(C-496/17 – Deutsche Post)*

Case C-345/17 – Proceedings brought by Sergejs Buivids, delivered on 14 February 2019. *(C-345/17 – Buivids)*

Case C-136/17 – GC and Others v Commission nationale de l'informatique et des libertés (CNIL), delivered on 24 September 2019. *(C-136/17 – GC and Others)*

Case C-507/17 – Google LLC, venant aux droits de Google Inc. v Commission nationale de l'informatique et des libertés (CNIL), delivered on 24 September 2019. *(C-507/17 – Google)*

Case T-738/16 – La Quadrature du Net, French Data Network, Fédération des Fournisseurs d'Accès à Internet Associatifs v European Commission [Case in progress]. *(T-738/16 – La Quadrature du Net and Others v Commission)*

Case C-311/18 – Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems [Case in progress]. *(C-311/18 – Facebook Ireland and Schrems)*

***Opinions of the Advocates General of the Court of Justice***

Opinion of Advocate General Mayras in C-48/69 – ICI v Commission, delivered on 2 May 1972.

Opinion of Advocate General Darmon in C-89/85 – Ahlström Osakeyhtiö and Others v Commission, delivered on 25 May 1988.

Opinion of Advocate General Trstenjak in C-585/08 and C-144/09 – Pammer and Hotel Alpenhof, delivered on 18 May 2010.

Opinion of Advocate General Jääskinen in C-131/12 – Google Spain and Google, delivered on 25 June 2013.

Opinion of Advocate General Cruz Villalón in C-230/14 – Weltimmo, delivered on 25 June 2015.

Opinion of Advocate General Bot in C-362/14 – Schrems, delivered on 23 September 2015.

Opinion of Advocate General Saugmandsgaard Øe in C-191/15 – Verein für Konsumenteninformation, delivered on 2 June 2016.

Opinion of Advocate General Szpunar in C-507/17 – Google, delivered on 10 January 2019.

***Canada***

Supreme Court of Canada – Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, [2017] 1 S.C.R. 824, delivered on 28 June 2017. *(SCC: Google Inc., v. Equustek Solutions Inc.)*

***France***

Tribunal de grande instance of Paris RG 05308 – Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France, 22 May 2000 *(LICRA v. Yahoo!)*

***Ireland***

The High Court – The Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems [2017] IEHC 545, delivered on 3 October 2017. *(The Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems)*

***United States***

United States Court of Appeals for the Second Circuit – United States v. Aluminum Co. of America, 148 F.2d 416 (2d Cir. 1945). *(Alcoa)*

Supreme Court of the United States – Hartford Fire Insurance Co. v. California, 509 U.S. 764 (1993). *(Hartford Fire Insurance)*

Supreme Court of the United States – Bartnicki v. Vopper, 532 U.S. 514 (2001). *(Bartnicki v. Vopper)*

District Court for the Northern District of California – Google LLC v. Equustek Solutions Inc., 2017 WL 5000834 (N.D. Cal. Nov. 2, 2017). *(N. D. Cal.: Google LLC v Equustek Solutions Inc.)*

**Official documents**

***Legislation***

*International agreements*

| | |
|---|---|
| UN Charter | Charter of the United Nations, signed on 26 June 1945. |
| ECHR | Convention for the Protection of Human Rights and Fundamental Freedoms, signed on 4 November 1950. |
| ICCPR | United Nations International Covenant on Civil and Political Rights (ICCPR), signed on 16 December 1966. |
| Convention 108 | Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, signed on 28 January 1981. |

*Primary EU law*

| | |
|---|---|
| TEU | Consolidated version of the Treaty on European Union, OJ C 326, 26 October 2012, p. 13–46. |
| TFEU | Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26 October 2012, p. 47–390. |
| Charter of Fundamental Rights | Charter of Fundamental Rights of the European Union, OJ C 326, 26 October 2012, p. 391–407. |

| | |
|---|---|
| Treaty of Lisbon | Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, OJ C 306, 17 December 2007, p. 1–230. |

*Secondary EU law*

| | |
|---|---|
| DPD, Data Protection Directive | Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. |
| Regulation 2271/96 | Council Regulation (EC) No 2271/96 of 22 November 1996 protecting against the effects of the extra-territorial application of legislation adopted by a third country, and actions based thereon or resulting therefrom. |
| Regulation 44/2001 | Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. |
| Regulation 2111/2005 | Regulation (EC) no 2111/2005 of the European Parliament and of the Council of 14 December 2005 on the establishment of a Community list of air carriers subject to an operating ban within the Community and on informing air transport passengers of the identity of the operating air carrier, and repealing Article 9 of Directive 2004/36/EC. |
| GDPR, General Data Protection Regulation | Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). |

*US legislation*

| | |
|---|---|
| US Constitution | Constitution of the United States, as amended. |
| US Sherman Act | Sherman Antitrust Act of 1890 (15 U.S.C. §§ 1–7). |

| | |
|---|---|
| EO 12333 | Executive Order 12333, 3 CFR, 1981 – United States intelligence activities, signed on 4 December 1981. |
| US SPEECH Act | Securing the Protection of our Enduring and Established Constitutional Heritage (SPEECH) Act of 2010 (Pub.L. 111−223, 124 Stat. 2380, H.R. 2765) |
| PPD-28 | Presidential Policy Directive – Signals Intelligence Activities, 17 January 2014. |
| CCPA | The California Consumer Privacy Act of 2018 (Assembly Bill No. 375 – Chapter 55 – An act to add Title 1.81.5 (commencing with Section 1798.100) to Part 4 of Division 3 of the Civil Code, relating to privacy). |

*Other legislation*

| | |
|---|---|
| UK Protection of Trading Interests Act 1980 | Protection of Trading Interests Act 1980 – 1980 CHAPTER 11 – An Act to provide protection from requirements, prohibitions and judgments imposed or given under the laws of countries outside the United Kingdom and affecting the trading or other interests of persons in the United Kingdom. |
| Yarovaya laws | Russian federal bills 374-FZ (Федеральный закон от 06.07.2016 г. № 374-ФЗ) and 375-FZ (Федеральный закон от 06.07.2016 г. № 375-ФЗ). |

***Official material of the European Union***

Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 15 October 1992. *(COM(92) 422 final – SYN 287)*

Proposal for a Regulation of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25 January 2012. *(COM(2012) 11 final)*

Communication from the Commission to the European Parliament and the Council, Rebuilding Trust in EU-US Data Flows, 27 November 2013. *(COM(2013) 846 final)*

Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, 27 November 2013. *(COM(2013) 847 final)*

Report from the Commission to the European Parliament and the Council on the second annual review of the functioning of the EU-U.S. Privacy Shield, 19 December 2018. *(COM(2018) 860 final)*

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. *(Commission Decision 2000/520/EC)*

Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. *(Commission Decision 2010/87/EU)*

Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data. *(Commission Implementing Decision 2012/484/EU)*

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. *(Commission Implementing Decision (EU) 2016/1250)*

Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council. *(Commission Implementing Decision (EU) 2016/2297)*

Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information *(Commission Implementing Decision (EU) 2019/419)*

Council Decision (EU) 2019/682 of 9 April 2019 authorising Member States to ratify, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. *(Council Decision 2019/682)*

Proposal for a Regulation of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Draft Version 56, 29 November 2011. *(Draft GDPR proposal 2011 (Version 56))*

EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, adopted on 16 November 2018. *(EDPB Guidelines 3/2018)*

EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection, 10 July 2019. *(EDPB-EDPS 2019)*

EDPS Opinion 4/2016 – Opinion on the EU-U.S. Privacy Shield draft adequacy decision, 30 May 2016. *(EDPS Opinion 4/2016)*

Official Journal of the European Union C 78, 29.2.2016. *(OJ C 78, 29.2.2016)*

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 9 November 2017. *(P7_TA(2014)0212)*

WP29 – Opinion 4/2000 on the level of protection provided by the “Safe Harbor Principles”, adopted on 16 May 2000*. (WP 32)*

WP29 – Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, adopted on 30 May 2002*. (WP 56)*

WP29 – Opinion 1/2008 on data protection issues related to search engines. *(WP 148)*

WP29 – Opinion 8/2010 on applicable law, adopted on 16 December 2010. *(WP 179)*

WP29 – Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain, adopted on 16 December 2015*. (WP 179 update)*

WP29 – Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc V. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12, adopted on 26 November 2014*. (WP 225)*

WP29 – Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016*. (WP 238)*

WP29 – Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, as last revised and adopted on 6 February 2018*. (WP 251 rev. 01)*

***Member State DPA material***

CNIL: Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against Google LLC. *(CNIL deliberation SAN-2019-001)*

ICO: Guide to the General Data Protection Regulation (GDPR), 22 May 2019, version 1.0.638. *(ICO Guide to the GDPR)*

***Non-EU material***

Privacy Amendment (Private Sector) Bill C2004B00628 (2000), Further Supplementary Explanatory Memorandum. *(C2004B00628)*

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) – Request by Uruguay to be invited to accede (GR-J(2011)10); 1118th meeting – 6 July 2011. *(Dec(2011)1118/10.3)*

UN – Report of the International Law Commission: Fifty-eighth session (1 May-9 June and 3 July-11 August 2006). General Assembly Official Records, Sixty-first session, Supplement No. 10 (A/61/10). *(ILC 2006)*

Public Consultation Issued by Ministry of Information, Communications and the Arts (MICA) of Singapore – Proposed Personal Data Protection Bill, 19 March 2012. *(MICA 2012)*

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). *(OECD Privacy Guidelines (1980))*

OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2006). *(OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy)*

The EU Data Protection Directive: Implications for the U.S. Privacy Debate. Hearing before the Subcommittee on Commerce, Trade and Consumer Protection of the Committee on Energy and Commerce, 8 March 2001, Serial No. 107-19. *(US Congress 2001)*

**Online sources**

Cnet: "Congress fears European privacy standards", 2 January 2002, accessed on 26 September 2019.
https://www.cnet.com/news/congress-fears-european-privacy-standards/
(Cnet 2002)

Speech of the European Commission Vice-President, EU Justice Commissioner Viviane Reding: "The EU data protection Regulation: Promoting technological innovation and safeguarding citizens' rights", 4 March 2014, accessed on 26 September 2019.
https://europa.eu/rapid/press-release_SPEECH-14-175_en.htm
(Reding 2014)

JD Supra: "The Right to Be Forgotten, Everywhere" by Albert Gidari, Jr on 5 June 2014, accessed on 26 September 2019.
https://www.jdsupra.com/legalnews/the-right-to-be-forgotten-everywhere-48744
(Gidari 2014)

World Economic Forum: "Do we need new laws for the age of cloud computing?" by Dan Jerker B. Svantesson on 3 February 2015, accessed on 26 September 2019.
https://www.weforum.org/agenda/2015/02/do-we-need-new-laws-for-the-age-of-cloud-computing/
(Svantesson 2015c)

Google: Blog post of 4 March 2016 – "Adapting our approach to the European right to be forgotten", accessed on 26 September 2019.
https://blog.google/around-the-globe/google-europe/adapting-our-approach-to-european-rig/
(Google 2016)

Human Rights Watch: “Russia: ‘Big Brother’ Law Harms Security, Rights”, 12 July 2016, accessed on 26 September 2019.
https://www.hrw.org/news/2016/07/12/russia-big-brother-law-harms-security-rights
(Human Rights Watch 2016)

C-Span: "Presidential Candidate Donald Trump Campaign Rally in Greenville, North Carolina" on 6 September 2016, accessed on 26 September 2019.
https://www.c-span.org/video/?414823-1/donald-trump-campaigns-greenville-north-carolina&start=408
(C-Span 2016)

Facebook: Newsroom Post of 17 April 2018 – "Complying With New Privacy Laws and Offering New Privacy Protections to Everyone, No Matter Where You Live", accessed on 26 September 2019.
https://newsroom.fb.com/news/2018/04/new-privacy-protections/
(Facebook 2018)

Microsoft: Blog Post of 21 May 2018 – "Microsoft’s commitment to GDPR, privacy and putting customers in control of their own data", accessed on 26 September 2019.
https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/
(Microsoft 2018)

DLA Piper: “California Consumer Privacy Act of 2018 (CCPA)”, October 2018, accessed on 26 September 2019
https://www.dlapiper.com/~/media/files/insights/publications/2018/10/mrs000113058-ccpa-slipsheet-v13ip.pdf
(DLA Piper 2018)

SAS: "Data Privacy: Are You Concerned? Insights from a survey of US consumers", 10 December 2018, accessed on 26 September 2019.
https://www.sas.com/content/dam/SAS/documents/marketing-whitepapers-ebooks/sas-whitepapers/en/data-privacy-110027.pdf
(SAS 2018)

nCipher: “Marking GDPR anniversary, nCipher survey reveals Americans’ data privacy attitudes”, 22 May 2019, accessed on 26 September 2019.
https://www.ncipher.com/about-us/newsroom/news-releases/marking-gdpr-anniversary-ncipher-survey-reveals-americans-data
(nCipher 2019)

US Congress: Nomination – PN260 – Keith Krach – Department of State 20 June 2019, accessed on 26 September 2019.
https://www.congress.gov/nomination/116th-congress/260
(US Congress 2019)

IAPP: "EU High Court hearings to determine future of Privacy Shield, SCCs" by Jennifer Baker on 25 June 2019, accessed on 26 September 2019.
https://iapp.org/news/a/eu-high-court-hearings-to-determine-future-of-privacy-shield-standard-contractual-clauses/
(Baker 2019a)

IAPP: "CJEU's hearing on Schrems II has both sides worried ruling could be sweeping" by Jennifer Baker on 9 July 2019, accessed on 26 September 2019.
https://iapp.org/news/a/cjeus-hearing-on-schrems-ii-has-both-sides-worried-ruling-could-be-sweeping/
(Baker 2019b)

European Law Blog: "The US, China, and Case 311/18 on Standard Contractual Clauses" by Peter Swire on 15 July 2019, accessed on 26 September 2019.
https://europeanlawblog.eu/2019/07/15/the-us-china-and-case-311-18-on-standard-contractual-clauses/
(Swire 2019)

CNIL: "'Right to be forgotten': the CJUE ruled on the issue", 24 September 2019, accessed on 26 September 2019.

https://www.cnil.fr/en/right-be-forgotten-cjue-ruled-issue
(CNIL 2019)

Wikimedia Foundation: "Do Europeans have a right to be globally delisted? The Court of Justice of the European Union says no." by Allison Davenport on 24 September 2019, accessed on 26 September 2019.
https://wikimediafoundation.org/news/2019/09/24/do-europeans-have-a-right-to-be-globally-delisted-the-court-of-justice-of-the-european-union-says-no/
(Davenport 2019)

Council of Europe: Chart of signatures and ratifications of Treaty 108 as of 26 September 2019, accessed on 26 September 2019.
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=cN6J4BCa
(Council of Europe 2019)

Merriam-Webster dictionary: “Reasonable”, accessed on 26 September 2019.
https://www.merriam-webster.com/dictionary/reasonable
(Merriam-Webster 2019)

European Commission: Standard Contractual Clauses, accessed on 26 September 2019.
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en
(European Commission – Standard Contractual Clauses)

European Commission: Adequacy decisions, accessed on 26 September 2019.
https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
(European Commission – Adequacy decisions)

## Abbreviations

| | |
|---|---|
| CJEU | Court of Justice [of the European Union] |
| CNIL | Commission nationale de l'informatique et des libertés |
| DPA | Data Protection Authority |
| DPD | Data Protection Directive |
| EDPB | European Data Protection Board |
| EDPS | European Data Protection Supervisor |
| EU | European Union |
| GDPR | General Data Protection Regulation |
| ICO | Information Commissioner's Office |
| ILC | UN International Law Commission |
| OECD | Organisation for Economic Co-operation and Development |
| UN | United Nations |
| US | United States |
| WP29 | Article 29 Data Protection Working Party |

# 1 Introduction

## 1.1 Blurring the territorial borders

It has long been the starting point in international law that a sovereign state is entitled to exclusively have control over the activity taking place on its soil, and that states should abstain from attempts to intervene in such internal affairs of each other.[1] For decades, such an approach has served mankind rather well – save for some uncertainties concerning, e.g., crimes taking place on state borders or on the high seas, the overall amount of jurisdictional conflicts has been rather low.

However, growing globalisation and especially the advent of the internet have permanently shaken this status quo. The amount of transnational trade activities keeps increasing, and more and more business are relying on processing of personal data as their key source of income. With the globalisation of data processing operations, an increasing number of parties are also taking interest in regulating the processing activities. Many states and other entities have been participating in such regulation by enacting strict and widely-applicable requirements concerning the processing and retention of personal data, demonstrating their divergent subjective interests in the matter – one can consider, for instance, the ambitious CCPA in California[2] and the somewhat questionable[3] Yarovaya laws in Russia[4] – in this respect, the EU is no exception.[5]

At the core of the issue is the difficulty of regulating online conduct: if states only regulated the activity taking place within their own territory, the level of protection provided to their citizens would be insufficient – online, individuals deal with a great amount of foreign companies that would not be covered by their home state's law, and forum shopping would be rather easy for the businesses engaging in online activity.[6] At the same time, however, if many states introduce legislation attempting to globally regulate the

[1] See the statements of 17th century Dutch jurist Ulrik Huber, who categorically claimed that a state's laws are only applicable within the state's territory and on every person within its territory (Bernhardt 1995, p. 338).

[2] For a review of the California Consumer Privacy Act, see DLA Piper 2018.

[3] See, e.g., Human Rights Watch 2016.

[4] For a review of the retention requirements under the Yarovaya laws, see Zhuravlev & Brazhnik 2018.

[5] For additional examples, see Svantesson 2013b, p. 113–122.

[6] It is not always even clear, what really constitutes an activity "within a certain territory" – is it the location of the subject or the object of the activity, or, perhaps, the equipment used that should be the decisive factor?

same type of activities, it might not be possible for those doing business online to adjust their activity to be compliant with every single applicable law. Unsolved, this problem could greatly complicate or even make it impossible to practice cross-border trade and other types of online business.[7] Consequently, a balance needs to be sought between guaranteeing the effectivity of a law regulating online activity and the sufficient level of protection of individuals online, and the reasonable approach to extraterritorial applicability of laws regulating cyberspace activities. Such balance is paramount in order to avoid a situation where compliance with all applicable legislation creates too much of a burden for businesses willing to engage in cross-border trade activities.[8]

The problem described above is especially relevant in the context of data protection law[9] – it is therefore important to investigate what actual effects the EU data protection regime has outside the EU borders in order to ensure its own efficiency. Furthermore, it is also important to review whether all of these effects are reasonable from the point of view of other states, which are, after all, primarily entitled to regulate the activity taking place within their territory. Such reasonableness assessment could help us develop better and more widely accepted ways of regulating data processing activities, which could, in the end, result in better protection for individuals in the EU and worldwide.

### 1.2 The aims, the research questions and the scope of this thesis

The aim of this thesis is to study the extraterritoriality of the EU data protection[10] law – particularly, how it is justified and how it is applied in practice outside the EU. As discussed later on, the GDPR has an exceptionally wide and somewhat vaguely defined territorial scope, which may be considered unreasonable by parties outside the EU and which may even clash with local legislation and values in non-EU countries.[11] The aims of this work are, on one hand, to identify the mechanisms of the GDPR which have an effect outside the EU, and, on the other hand, assess whether they are reasonable from

[7] Ryngaert 2015a, p. 74–75, Svantesson 2013b, p. 21–22.

[8] See Svantesson 2013a, p. 278.

[9] While data protection law regulates all data processing activities, not only the ones taking place in an online environment, most of the territorial issues associated with cross-border data processing activities are, indeed, characteristic to the processing of personal data taking place online.

[10] While the core meaning of the right to privacy and the right to the protection of personal data is not identical (see, for instance, the differences in Articles 7 and 8 of the Charter), for the purposes of this work, I will use the concepts of privacy and data protection synonymously, unless the context specifically implies otherwise.

[11] See, e.g., Wimmer 2018, p. 571.

the perspective of non-European parties. The research questions of this work can therefore be formulated as follows:

(1) What are the extraterritorial mechanisms of the EU General Data Protection Regulation?

(2) Are all of the extraterritorial mechanisms identified above in question (1) reasonable from the perspective of international law?

The scope of the EU data protection law has often been regarded as extraterritorial[12] – however, there are numerous different definitions to what is actually referred to when one speaks about "extraterritoriality". With ambiguity concerning the definition of extraterritoriality comes the confusion regarding its justification: by enacting requirements that have an effect outside the state borders, the regulator, at least to some extent, contests other states' sovereignty and sole authority to regulate the conduct taking place on their territory.[13] How should such an encroachment be legitimised, and when do such extraterritorial claims go too far to be accepted by other states? Due to these uncertainties, before it is possible to evaluate the extraterritorial mechanisms of the GDPR, it is first necessary to assess on a general level the different definitions of extraterritoriality and certain issues related thereto – namely, how extraterritorial assertions should be justified and how they can be enforced.

These questions concerning extraterritoriality as a phenomenon will be reviewed in section 2, at the beginning of which I will briefly look into the concepts of state sovereignty and jurisdiction. After this, I will examine in further detail the definition of extraterritoriality and certain different issues and debates related thereto in order to create a robust framework for the assessment of the extraterritorial claims made in the GDPR. Only after establishing the findings concerning extraterritoriality in general, it is possible to apply them in the context of the EU data protection law and evaluate, to which extent the EU data protection law is extraterritorial, and to which extent these extraterritorial assertions and effects are reasonable. In section 3, I will look in further detail into the extraterritoriality of EU data protection legislation, focusing on the extraterritorial mechanisms of the GDPR itself and considering, where applicable, the interpretations of rel-

[12] See, e.g., Greze 2019, Azzi 2018, Kuner 2015a, Svantesson 2015a, Van Alsenoy & Koekkoek 2015.

[13] Gerber 1984, p. 212.

evant provisions of the DPD. Following this review, in section 4, I will assess the reasonableness of the extraterritorial mechanisms of the GDPR from the point of view of international law, examining the findings of section 2 in the context of EU data protection law and the arguments presented from an European perspective in order to justify the Regulation's extraterritoriality. At the end of this work, after identifying certain issues with the extraterritoriality of the GDPR, I will examine some different approaches to the subsequent development and interpretation of the EU data protection law in order to improve its extraterritorial flexibility and reasonableness.

As the focus of this work is a general discussion concerning the extraterritorial nature of the GDPR, I will not examine the multitude of specific situations and scenarios where the GDPR could apply outside the EU in connection with question (1).[14] Instead, based on the text of the provisions and the relevant case law, I will look into the extraterritoriality of the GDPR on a more general level, highlighting the specific mechanisms that give the GDPR its extraterritorial effect and reviewing the relevant case-law concerning these mechanisms in order to establish the current extraterritorial extent of the GDPR.

Additionally, it should be noted at this point that some ambiguity might be related to question (2) as its aim is to assess the reasonableness of the extraterritoriality of the GDPR – the word ”reasonable” carries multiple different meanings ranging from rationality to moderateness.[15] For the purposes of this work, I will focus on the concept's latter dimension, as I will examine the moderateness and fairness of the EU data protection law. Therefore, it is not my intention to question the legitimacy of the EU data protection law as a whole – instead, I will examine the justification of the extraterritorial effects of EU data protection law, considering, *inter alia*, how fair the assertions are from the point of view of all other non-EU states, whether the assertions are proportionate, well-founded, and predictable. In my review, I will also take into account the differences between making an extraterritorial assertion in the legal text and the enforcement of such an assertion, highlighting the enforceability as one of the criteria determining the reasonableness of an assertion. When seeking an answer to question (2), the interests of other states will be examined and weighed against the EU's interests in order to determine the possible limitations to the extraterritorial application of the EU data protection requirements.

[14] The EDPB has made an assessment of specific example scenarios in the EDPB Guidelines 3/2018.
[15] Merriam-Webster 2019.

### 1.3 Methods

The nature of the research questions of this work is twofold: in question (1), I will identify the prevailing extraterritorial effects of the current EU data protection law, and in question (2), I will evaluate their reasonableness by assessing their justification and effectivity. For this reason, different research methods[16] will be assumed in order to properly review both of these questions.[17]

The main aim of question (1) is to clarify the current content of law – therefore, a doctrinal method will be assumed in order to review it, as the aim of clarifying the content of law in force is at the core of doctrinal research.[18] In Finnish legal research, doctrinal method has been traditionally divided into its practical and theoretical counterparts, with the former focusing on the interpretation of normative material and the latter focusing on its systematisation.[19] Despite this division, the use of both of these elements, at least to a certain extent, will be visible over the course of this work when assessing question (1)[20] – by the means of the primary practical doctrinal method, I will interpret the relevant provisions, along with applicable case law and other sources of law, in order to assess whether an effect outside the EU is achieved; whereas by means of the theoretical doctrinal method, I will organise the different extraterritorial effects and assertions of the GDPR based on their severity and impact and create an overall picture of the extraterritoriality of the GDPR.

As the first research question concerns primarily the content of the secondary EU law, its characteristic features will affect this doctrinal research, which is why teleological arguments often preferred by the CJEU are awarded a high priority in the interpretation of the provisions of the GDPR.[21] Additionally, the specifics of the hierarchy of legal

[16] Methods in legal research can be considered as a type of tools or frameworks for the assessment of research question established in different branches of law. This framework may place emphasis on different matters and should be selected individually based on the nature of the question (Hirvonen 2011, p. 4–5).

[17] At the beginning of the work, I will also look into the meaning of the concept of extraterritoriality, as well as certain other international law concepts related to it. This review, however, will serve as a groundwork for the review of the actual research questions; hence, no specific method will be assumed for the review of the concept of extraterritoriality. However, the source material used for this review will be discussed in the next section.

[18] Neergaard & Nielsen 2011, p. 105; Hirvonen 2011, p. 22.

[19] Hirvonen 2011, p. 25.

[20] See Aarnio 1997, p. 36–37.

[21] While teleological arguments are not the only ones used in doctrinal research of EU law, they are most prominent ones (see Talus & Penttinen 2015, p. 16). Teleological interpretation of EU law can be seen connected with the *effet utile* of EU law (Reichel 2018, p. 114, 122–123).

sources in EU law is to be considered – secondary law, such as the GDPR itself, are to be interpreted in the light of primary EU law, i.e., the TEU, the TFEU and the Charter, and in accordance with the relevant CJEU case law.[22] It should be noted that while there are various national-level provisions concerning the protection of personal data even within the EU,[23] the first research question concerns specifically the extraterritoriality of the general requirements of the GDPR.[24] As the GDPR is equally binding in all Member States,[25] national legislation concerning the protection of personal data will not be reviewed, and the nature of the research will be specifically EU-doctrinal.[26]

However, as it will be discussed later on, not all effects of EU data protection law stem directly from the specific provisions of the GDPR – some of the extraterritorial effects have a much more subtle effect caused by, among other things, the EU's cooperation with other states in the field of data protection and, in some instances, the mere existence of a high-level data protection regime set in place by the EU. The extent of the extraterritorial effect in these cases will be examined by taking into account a wider perspective examining the relationship between law and society, i.e., the effect of EU data protection regime on non-European persons and states on a larger scale.[27]

Another variation of doctrinal research is adopted when reviewing the question (2). As the aim of the second question is to assess the reasonableness of the extraterritorial assertions of the EU data protection law, a mere descriptive examination of the content of these assertions is no longer sufficient. Therefore, the while the method assumed for the review of the second question remains doctrinal, it will take on a critical dimension. The focus of critical doctrinal research is to examine the content of current legal norms

[22] See, e.g., Riesenhuber 2017, p. 251. The source material used throughout this work will be further reviewed in the next section.

[23] National data protection laws of the EU Member States concern specific clarifications to or derogations from the provisions of the GDPR, where such are allowed – the core principles of the GDPR remain the same throughout the Union (see Recital 8 of the GDPR).

[24] The autonomous nature of EU law as a legal order has been affirmed in C-26/62 – *Van Gend en Loos*, where the Court found that "the community constitutes a new legal order of international law for the benefit of which the states have limited their sovereign rights. (…) Independently of the legislation of member states, community law therefore not only imposes obligations on individuals but is also intended to confer upon them rights which become part of their legal heritage". See also Reichel 2018, p. 109.

[25] Köndgen 2017, p. 138.

[26] It should also be emphasised that this thesis focuses specifically on the examination of EU law. For this reason, even though I will examine certain legislative aspects from outside the EU, especially in section 2 concerning the concept of extraterritoriality, the examination will not constitute a comparative study examining the differences between the jurisdictions concerned.

[27] Hirvonen 2011, p. 29; see also Tuori 2000, p. 317.

critically from an internal perspective, and the normative scale for the assessment will be based on the principles found within the legal system itself.[28] For the purposes of this work, I will review the extraterritorial mechanisms of the GDPR from the viewpoint of the principles of public international law.[29] Further emphasising the use of a critical doctrinal approach, at the end of this work several different propositions will be discussed as possible solutions to the potential difficulties faced by the extraterritoriality of the GDPR.[30]

However, a normative scale founded purely on the criteria found within the legal system will not necessarily be sufficient for the assessment of the extraterritorial mechanisms of the GDPR, as exercise of extraterritorial jurisdiction is a subject that can strongly split politically polarised opinions. Extraterritorial assertions, even if they are made with good intentions, can be viewed as a show of power or even imperialism,[31] and can, at worst, even spark a diplomatic crisis.[32] For this reason, while law and politics is not the core method for the review of the second question and while the political arguments will not form the base for the critical evaluation of the GDPR, certain political viewpoints will be taken into account insofar as they are relevant for the evaluation of the effects of the GDPR. These political arguments will, however, be kept separate from critical doctrinal assessment of extraterritoriality.

### 1.4 Source material

As the first question is deeply rooted in EU law, the systematics and the hierarchy of legal sources in EU law will be acting as a basis throughout this work.[33] The main

[28] Hirvonen 2011, p. 50; Määttä 2015, p. 36; see also Tuori's theory of critical legal positivism, Tuori 2000, p. 325, 342.

[29] It has been argued that data protection law is located at the boundary of public and private international law (Bygrave 2000, p. 252). However, its belonging to each of these groups is contextual – when the matter concerned is the activity of a private actor, such as the signing of a data processing agreement, the framework selected should focus more on the private international law. However, in this case I will be reviewing the general assertions of jurisdiction made by the EU in the GDPR, and, consequently, the assessment framework will be based on public international law (Kuner 2010a, p. 183)

[30] Kolehmainen 2015, p. 2–3.

[31] Zielonka 2008, p. 475.

[32] Brownlie 2008, p. 304. A great deal of literature concerning extraterritorial assertions of jurisdiction has been released in the field of political science, see, e.g., Emmenegger & Eggenberger 2018 examining the political aspects of the US using its market power to penetrate through the Swiss banking secrecy.

[33] It has even been argued that the doctrinal method in EU law can, in fact, be seen as less of an independent method and more of a specific type of approach to different sources of EU law that is to be combined with other methods (Reichel 2018, p. 109).

sources of EU law are the primary and secondary legislation.[34] The primary law – namely, the TEU, TFEU and the Charter of Fundamental Rights[35] – is at the top level of the hierarchy of legal sources, and, as noted above, the core principles laid down in these instruments guide the consequent interpretation of lower-level sources of law.[36] Secondary law includes the regulations, directives and decisions enacted by the EU. These norms contain most of the subject matter provisions of EU law, and they can be seen as specifying the content of the general principles expressed in the primary law.[37] The GDPR, being a regulation, belongs to this group of legislative instruments, and its foundation in the primary EU law is acknowledged in Recital 1 of the Regulation.[38]

While the secondary law provides specification to the principles contained in the primary norms, this level of precision is often not enough on a practical level. The interpretation of the secondary norms is therefore assisted by the case law of the CJEU – while the Court's reasoning and decisions do not have a formally binding nature, in practice, the interpretations of the Court become part of the binding law.[39] Additional assistance in the interpretation of the GDPR (and, where relevant, the DPD) is also provided by the preparatory and explanatory documents relating to the GDPR and the DPD,[40] and by the opinions, guidelines and other instructions of the WP29 and the EDPB. While these documents lack binding nature, CJEU Advocates General have referred to them in their reasoning.[41]

While these normative sources, along with academic writings and DPA guidance concerning the matter, will form the base of argumentation in relation to the first research

[34] Köndgen 2017, p. 120.

[35] As of 2009, the Charter was given legal status as primary EU legislation pursuant to Article 1 of the Treaty of Lisbon (see amended Article 6 TEU).

[36] Even inside the primary law, a hierarchical structure can be observed: it has been argued that the principles contained in Article 2 TEU serve as a basis for the entirety of the EU legal system, and with all other primarily law being based on these principles (Talus & Penttinen 2015, p. 4).

[37] Article 288 TFEU. Raitio 2016, p. 203. While the legal status of the recitals of secondary law is somewhat unclear, it has been concluded that they cannot be given same independent and binding character as the provisions of these instruments (Köndgen 2017, p. 141–142).

[38] As reasoned above, while the field of data protection is also regulated on a national level within the EU, only the EU law instruments will be examined over the course of this work.

[39] Article 267 TFEU; Talus & Penttinen 2015, p. 8. The legal status of the opinions of Advocates General is less significant, as the views expressed in the opinions do not bind the Court – the reasoning in these opinions, however, can provide additional help in the interpretation of EU law (Raitio 2016, p. 136).

[40] However, as will be discussed later on, the explanatory documents offer little help in the evaluation of the territorial scope of the GDPR.

[41] See, e.g., Opinion of Advocate General Szpunar in C-507/17 – *Google*, delivered on 10 January 2019, para 34.

question, when evaluating the reasonableness of EU law and the effect of its extraterritorial assertions, the use of these purely normative sources will not be sufficient. For this reason, these sources will, at least to some extent, give way to the social and political arguments concerning the extraterritorial impact of the EU data protection law.

Additionally, the normative sources of EU law will not be helpful in section 2, where I will lay the groundwork for the assessment of the research questions by clarifying the definition of extraterritoriality and other relevant international law concepts. While this is not a discrete research question *per se*, specific type of source material is still needed to address the matter. Due to, on one hand, the inherent decentralised nature of international law and the lack of legislative instruments comparable to, e.g., national constitutions,[42] and, on the other hand, the non-normative nature of the concept of "extraterritoriality",[43] there will likely be as many definitions to extraterritoriality as there are commentators looking into its definition. The process of reviewing the different definitions is essential in order to find a the one best suited for the purposes and subsequent research questions of this work.[44] As the character of the issues concerned when examining data protection law is rather novel, the approach to defining and justifying extraterritoriality that will be assumed will also be modern and practical.

# 2 Jurisdiction and extraterritoriality in international law

## 2.1 Sovereignty

Before I begin the examination of extraterritoriality as a concept, it is useful to briefly examine the many-sided concept of sovereignty,[45] as broad extraterritorial claims of certain states can sometimes be considered infringements on other states' sovereignty and thereto related privileges.[46] Sovereignty is often used as a term describing a state's power to act independently and without external control in different circumstances, and

[42] Currie 2008, p. 4; McConville & Chui 2017, p. 254.

[43] See, e.g., Svantesson 2013b, p. 83–85.

[44] When discussing extraterritoriality, the importance of critical reading of academic material cannot be overstressed. Due to its highly politicised nature, there are numerous commentators viewing extraterritorial assertions as either inherently unacceptable or, on the opposite, completely permissible (for instance, US commentators tend to critically view the EU data protection law as exorbitant or even unacceptable under international law, see, e.g., Lam 2017, p. 10).

[45] Crawford 2012, p. 448; Svantesson 2013b, p. 77–81.

[46] Perritt 2000, p. 892.

it may also include certain responsibilities and internal and external aspects.[47] It is also possible to differentiate between the internal and external aspects of sovereignty, i.e., the freedom of internal self-determination and external independence from other states respectively.[48]

With multiplicity of different definitions and meanings, the various understandings of sovereignty have also been thoroughly criticised. Being an abstraction and simplification of reality, the meaning of the term remains rather ambiguous and context-specific.[49] However, as this work focuses on extraterritorial legislation and thereto related limitations, I will concentrate on the aspect of sovereignty that relates to the sovereign state's sole authority to practise, within its own geographical territory, the functions that belong to it as a sovereign state.[50]

Even more uncertainties arise when the context of sovereignty is applied in the EU context. The EU, being a *sui generis* union of sovereign states,[51] is not a sovereign state itself in its traditional meaning and lacks some of the competences that are often considered a part of state sovereignty[52] – the EU's competences are limited to those granted to it by the Member States, and, consequently, EU has no competence-competence.[53] Consequently, the EU Member States acting together behind the EU retain their status as independent sovereign states.

However, when examining the EU as an actor in the international field, it is clear that it bears many similarities with other "conventional" sovereign states – under Article 47 TEU, the EU has legal personality, which has been internationally recognised.[54] While

---

[47] Fox 1997, p. 293–294; Endicott 2010, p. 245; Crawford 2012, p. 447. See also Endicott 2010, p. 245, according to whom sovereignty consists, on a basic level, of the state's absolute power within a community, absolute independence externally from other states and full power as a legal person in international law.

[48] Koskenniemi 2005, p. 240–241.

[49] Crawford 2012, p. 448. Koskenniemi goes as far as stating that due to its ambiguity, sovereignty indeed does not have – and cannot be given – any fixed meaning or "natural extent" that could be always applicable (Koskenniemi 2005, p. 242).

[50] *Island of Palmas Case*, p. 838. This can be seen to include, on one hand, the state's right to exclude other states from practising such functions within its borders and, on the other hand, the state's obligation to protect the rights of other states within the state's own territory.

[51] See also Petkova 2018, p. 1136, describing the EU as a "quasi-federated entity".

[52] This transfer of rights is referred to as the *principle of conferral*, Raitio 2016, p. 215–216; see also Köndgen 2017, p. 119.

[53] See Tiilikainen et al. 2005, p. 34, discussing competence-competence of the EU in the context of the then-relevant Treaty establishing a Constitution for Europe

[54] Hijmans 2016, p. 467, 505.

the EU does share its regulatory competence with the Member States in the field of data protection,[55] the binding and significant nature of the GDPR makes the EU itself as "the principal – if not sole – actor" representing the Member States in this field.[56] Additionally, as I will be specifically focusing on the assertions of jurisdictions made by the EU,[57] the encroachments on the "sovereignty" of the EU will not be discussed here. Thus, while the EU is not a sovereign state *per se*, from an external perspective, the EU can still be compared to other independent sovereign legislators in the field of data protection. While the core differences between the EU and other sovereign states should be borne in mind, they will not substantially affect the course of this work.

In light of the meaning of sovereignty reviewed above, it is clear that when a regulator attempts to influence conduct outside its borders, it intrudes, at least to some extent, into the realm of exclusive rights and freedoms of another states, i.e., an encroachment of another state's sovereignty takes place.[58] In this context, it is also relevant to briefly examine the principles of comity and sovereign equality. While not a legal obligation, comity refers to a principle according to which "States respect each other's policy choices and interests in a given case, without inquiring into the substance of each other's laws".[59] In accordance with the principle of comity, states should therefore refrain from trying to control such activity that another state is better suited to regulate.[60] The principle of sovereign equality serves a similar purpose – while it does not imply a *de facto* equality of power between different sovereign nations, it refers to the "equal courtesy", with which all states should treat each other.[61] It should also be noted that this principle does not refer to a scenario in which a majority of states could impose their views on a minority – therefore, the EU Member States all together as sovereign entities are not entitled to impose their data protection views on a single non-EU state.[62] As it

[55] See Article 4 TFEU.

[56] Hijmans 2016, p. 467.

[57] As opposed to the ones made against the EU.

[58] Gerber 1984, p. 212.

[59] Ryngaert 2015b, p. 147.

[60] Ryngaert 2015b, p. 148.

[61] Instead, it signifies an equality of rights and status in comparison with other nations, including the right to retain exclusive authority within its territory, "regardless of disparities in economic or military power" (Muse 1996–1997, p. 241–242; see also Ryngaert 2015b, p. 6).

[62] Lowe 2007, p. 114–116. A comparison can be made to decision-making in international organisations: does sovereign equality refer to the "one country, one vote" principle used in, e.g., the UN General Assembly (Article 18(1) of the UN Charter), or does the state population play a decisive role, like it does in the EU Parliament (Article 14(2) TEU)? Neither of these approaches can, however, be directly applied outside international organisations: the latter approach could imply, for instance, that the most populous states, such as China, could be entitled to impose their views on all smaller states.

will be discussed later on, these principles should be considered when attempting to regulate phenomena with a naturally-occurring cross-border character, such as online activities.[63]

## 2.2 Jurisdiction

As with sovereignty discussed above, there is no single correct and exhaustive definition for jurisdiction, either.[64] However, in general, jurisdiction can be defined to mean the extent of a state's right[65] and ability to "regulate conduct or the consequences of events",[66] and it is, indeed, closely linked to state sovereignty.[67] There are multiple different specific activities that fall under the scope of the umbrella term "jurisdiction", with the use of legislative power being just one of such activities. Jurisdiction can, therefore, as it is classically viewed, concern (i) the state's power to enact legislation (legislative or prescriptive jurisdiction), (ii) the state's power do adjudicate a certain matter (judicial or adjudicative jurisdiction), or (iii) the state's power to enforce its law (enforcement or executive jurisdiction).[68] Each of these types of jurisdiction can be exercised extraterritorially.[69]

In addition to the multiple dimensions of jurisdiction, there are multiple different principles based on which jurisdiction can be asserted. Consequently, states may assume jurisdiction over an event based on, e.g., the territory where it occurred, nationality of

---

[63] Bauchner 2000, p. 715; Kuner 2015a, p. 245. Both of these principles can also be seen to apply to the EU as a regulator in the international field.

[64] Akehurst 1972–1973, p. 145.

[65] Or, in the case of the EU, a regulator's right transferred to it by the Member States.

[66] Oppenheim et al. 1996, p. 456. Other definitions are naturally possible, however, jurisdiction on a general level is often defined specifically through the allocation and claims of competence to control different activities, relationships and phenomena (see Capps et al., 2003 p. xix and Berman 2003, p. 3).

See also Kuner 2010a, p. 178–179, defining jurisdiction as "the State's right under international law to regulate conduct in matters not exclusively of domestic concern" – some definitions therefore assume that the term "jurisdiction" inherently includes a sort of conflict of jurisdictions, i.e., even the slight possibility of several states willing to assert jurisdiction over a matter. This definition might be appropriate, though, since, as it will be discussed later, in an increasingly globalised economy, even the smallest actions can have global effects, in which case there remain very few matters that can be considered of a certain state's "exclusive domestic concern".

[67] Mann 1973, p. 22. See notes concerning sovereignty of the European Union above in section 2.1.

[68] See, e.g., Kuner 2010a, p. 184; Ryngaert 2015b, p. 9–10; Coughlan et al. 2007, p. 32 and Akehurst 1972–1973, p. 145. Svantesson additionally points out that a separate type of jurisdiction may concern the state's power to investigate a certain matter (investigative jurisdiction, see Svantesson 2013b, p. 67–68), and, according to Ryngaert, certain states have their own special type of limited jurisdiction over the activities in the states' maritime zones and even on the high seas (functional jurisdiction, see Ryngaert 2015a, p. 58).

[69] Svantesson 2013b, p. 67–68.

the parties concerned, or the extent of the consequences of the event.[70] The traditional principles for basing jurisdiction are discussed in the 1935 Research Draft Convention on Jurisdiction with Respect to Crime,[71] and, in practice, no substantial changes have taken place since the publication of the draft.[72] While in accordance with their definitions, many of these principles are especially relevant in the context of criminal law with a clearly defined "perpetrator" and "victim". However, essentially all of these principles can also be applied in a civil law context.[73]

The Harvard Draft identifies a total of five[74] principles for basing jurisdiction: the first and foremost principle is the (subjective) territoriality principle, under which, as it has been traditionally viewed, the state has exclusive authority and jurisdiction over events taking place within its geographical territory.[75] In addition, while not part of the Harvard Draft list,[76] the *objective* territoriality principle, concentrating on events taking place at least partially within a state's territory, can also be highlighted as a separate principle for basing jurisdiction.[77] However, as it will be discussed later, in the ubiquitous online world,

---

[70] See, e.g., Azzi 2018, p. 131.

[71] Harvard Draft 1935.

[72] Svantesson 2014, p. 80–81; see also, e.g., Kuner 2010a, p. 188–191 and Brownlie 2008, p 300–306. For the purposes of this work, I will assume a slightly different approach to assertions of jurisdiction, since, as it will be discussed below, the Harvard Draft principles can be considered outdated in the era of the internet. Nevertheless, as these principles form the traditional international law understanding of jurisdiction, it is useful to briefly examine them.

[73] Even though non-criminal jurisdiction is "formally civil", it often involves coercive and penal elements – the situation is similar in the case of data protection law. See Kuner 2010a, p. 188; Mann 1973, p. 30–31; Brownlie 2008, p. 300; Currie 2008, p. 333–334.

[74] Harvard Draft 1935, p. 445. While the Harvard Draft lists only five principles, according to Svantesson, the draft actually covers six, as the subjective and objective territoriality principles should be treated separately (Svantesson 2014, p. 81)

[75] Buxbaum 2009, p. 636. The subjective territoriality principle has been, without a doubt, the primary principle of basing jurisdiction during the past decades, and it is universally recognised all over the world (Ryngaert 2015a, p. 55–56).

[76] Svantesson 2014, p. 81.

[77] As opposed to subjective territoriality, the later-developed objective territoriality is a principle for certain criminal cases where an offence has taken place abroad, but an "essential constituent element of a crime" takes place within the territory of the state asserting jurisdiction (Crawford 2012, p. 458–459; Buxbaum 2009, p. 636; Bernhardt 1995, p. 341. As argued by Svantesson, objective territoriality can also be applied to non-criminal non-compliance – according to him, Article 4(1)(c) DPD was based on this principle, as the assertion of jurisdiction was based on the location of equipment used in data processing; see Svantesson 2013b, p. 142).

Objective territoriality principle was adopted in the *Lotus* case, which paved the way for the growing use of objective territoriality as a basis for asserting jurisdiction. The *Lotus* case concerned a collision between a French mail steamer and a Turkish cargo ship causing the Turkish ship to sink and killing eight crew on board. After the collision, Turkey claimed criminal jurisdiction over the watch duty officer of the French ship, allegedly responsible for the death of eight Turkish nationals aboard the Turkish ship. France stated that Turkey had no jurisdiction over the French officer, but, according to the PCIJ, France had to show that Turkey's assertion of jurisdiction violated some specific rule of international law. As no rules were violated, Turkey was granted jurisdiction over the case, despite

it may not even be possible to define a location of an event, suggesting that in this respect, the principles of territoriality may be nearing their obsolescence. Other principles identified in the Harvard Draft are the active personality principle[78], the protective principle,[79] the universality principle[80] and the passive personality principle,[81] in the general order from the most universally accepted to the most controversial.[82]

In addition to these six principles, and as an extended variation of the objective territoriality principle,[83] the effects doctrine can be assumed. According to the effects doctrine, a state may assert jurisdiction over a certain event or conduct taking place abroad when

---

the flag state of *Lotus* being France. In the judgment, the PCIJ formed two generally accepted principles: (i) a state may not exercise jurisdiction on the territory of another without its consent, and (ii) a state may claim jurisdiction abroad if a reasonable contact exists between the subject of the case and the state asserting jurisdiction (*The Case of SS Lotus;* Bernhardt 1995, p. 339–340; Raustiala 2009, p. 106; Crawford 2012, p. 459).

[78] Originally mentioned in the Harvard draft as the "nationality principle". However, for the sake of clarity of the comparison with the passive personality principle, I have assumed the term "active personality principle" used by, e.g., Ryngaert (see Ryngaert 2015b, p. 104).

On the basis of the active personality principle (i.e., the nationality principle), a state may assert jurisdiction over a case where the perpetrator is a national of that state, despite him or her being located abroad. The use of the active personality principle is seen as a mark of allegiance of nationals to the state, and, thus, can be considered as an element of sovereignty (Crawford 2012, p. 459–460; Brownlie 2008, p. 303). The principle is typically applied only in the case of the most serious crimes, where it is recognised that there might be a need to establish their penalisation in case the domestic authorities in the state of perpetration fail to do so (Ryngaert 2015b, p. 104–106, Crawford 2012, p. 460).

[79] The protective principle allows a state to assert jurisdiction in order to protect itself from harmful activity abroad. Traditionally, this principle has concerned specifically the protection of the state itself, including its sovereignty and independence, and not the protection of the citizens of the state. Being a diplomatically controversial principle, it is rarely applied in practice (Kuner 2010a, p. 190; Ryngaert 2015b, p. 114, 116; Wimmer 2018, p. 558).

[80] Based on the universality principle, a state can essentially assume jurisdiction over a specific matter with no factual link between the state and the matter or its parties (Ryngaert 2015b, p. 126). Such assertions have often been related to, e.g., piracy, drug trafficking, and other serious crimes with an international nature and that are so serious that "all mankind has a legitimate interest in repressing them" (Lowe 2007, p. 177). Universal jurisdiction is often established by the means of international conventions (Akehurst 1972–1973, p. 160–161).

[81] The passive personality principle allows a state to assert jurisdiction over a case based on the nationality of the victim of the illegal conduct. The principle is based on a state's legitimate interest to assert jurisdiction over a case involving its national as a victim; however, it is unclear whether such interest constitutes a proper jurisdictional link for the assertion to be acceptable and to outweigh the other states' potential assertions based on more common principles (Wimmer 2018, p. 558; Ryngaert 2015b, p. 110; Brownlie 2008, p. 304).

[82] Harvard Draft 1935, p. 445. It should be noted that justification of an extraterritorial assertion does not automatically follow the applicability of these principles (Wimmer 2018, p. 559). As it will be discussed below, assertion should always be justified separately considering all relevant factors, and the applicability of the Harvard Draft principles can be viewed as just one of the factors justifying an assertion.

[83] Bernhardt 1995, p. 341. As principles for basing jurisdiction presented above may overlap, the effects doctrine can also be seen to be related to, e.g., the passive personality or the protective principles, as both of these also deal with certain kinds of domestic effects caused by conduct that takes place abroad (see also Svantesson 2014, p. 83).

said event has some effects within the territory of the state making the assertion.[84] The use of the effects doctrine can be extended to apply to many fields of law, and it has been developed in competition law where anti-competitive behaviour has caused negative effects of outside the state, in which the behaviour initially took place.[85] The scope of the effects doctrine is also wider in so far as it does not set strict requirements concerning the personal or territorial connection of parties to the state asserting jurisdiction.[86] As it will be discussed later on, the targeting criterion under Article 3(2) GDPR can be considered to be based, at least partially, on the effects doctrine.

However, exaggerating, one could even argue that the effects doctrine lets basically any willing state to assume jurisdiction over a case, as "everything has an effect on everything".[87] Such assertions could, after all, cause certain states' jurisdiction to expand excessively encroaching on the exclusive sovereign rights and freedoms of other states.[88] Additionally, as the effects doctrine as a basis for jurisdiction has never been

---

[84] Kuner 2010a, p. 190; Ryngaert 2015b, p. 83–84; Svantesson 2013b, p. 136–137.

[85] For decades, the US was famous for its broad territorial assertions based on the use of the effects doctrine – after the enactment of the US Sherman Act, the US' extraterritorial assertions in the field of competition law became commonplace (Raustiala 2009, p. 111, 113). For instance, in *Alcoa* case, the US Court of Appeals for the Second Circuit distanced itself from strict territoriality and was the first to adopt the doctrine in a civil matter (Senz & Charlesworth 2001, p. 81), stating that "any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends" (*Alcoa,* p. 443; see also Bernhardt 1995, p. 340; Raustiala 2009, p. 102–103). Similar approach was later assumed by the US Supreme Court in *Hartford Fire Insurance* (*Hartford Fire* Insurance, p. 796; see also Sufrin 2003, p. 106).

Widespread assertions by the US also prompted as wave of blocking legislation enacted by the states affected by the US' assertions in order to mitigate their effects (Raustiala 2009, p. 115–116, Developments in the Law: Extraterritoriality 2011, p. 1255. For examples of blocking legislation, see the UK Protection of Trading Interests Act 1980, or Regulation 2271/96).

At first, the EU was reluctant to apply the effects doctrine, as demonstrated in the *Dyestuffs* Case (C-48/69 – *ICI v Commission*) and the *Wood Pulp Case* (C-89/85 – *Ahlström Osakeyhtiö and Others v Commission*; cf. Opinion of Advocate General Mayras in C-48/69 – *ICI v Commission*, delivered on 2 May 1972, p. 685 and Opinion of Advocate General Darmon in C-89/85 – *Ahlström Osakeyhtiö and Others v Commission*, delivered on 25 May 1988, para 44, in both of which Advocates General did support the use of the effects doctrine; see also Gerber 1983, p. 756; Layton & Parry 2004, p. 319–321; Capps et al. 2003, p. 110–111). However, as the economic power of the European Union grew, the EU also embraced the effects doctrine (Scott 2014b, p. 88). The effects doctrine was openly adopted in *Gencor v. Commission* (T-102/96 – *Gencor v Commission*, para 90 et seq.).

[86] Svantesson 2014, p. 83.

[87] Kuner 2010a, p. 190.

[88] Bernhardt 1995, p. 341–343. This is especially problematic in the case of civil law, as different states may have different intentions when regulating economic matters.

However, the issue has already been addressed in the *Alcoa* case mentioned above, in which the Second Circle concluded that "There may be agreements made beyond our borders not intended to affect imports, which do affect them, or which affect exports. *Almost any limitation of the supply of goods in Europe* (…) *may have repercussions in the United States if there is trade between the two*. Yet when one considers the international complications likely to arise from an effort in this country to

defined comprehensively, its meaning has always been somewhat vague. Mann, for instance, considered the effects doctrine exorbitant by its nature[89] – such an approach, however, can no longer be considered appropriate in a world where globalisation and cross-border business activity is constantly growing. For this reason, a more nuanced, sophisticated and case-specific approach should therefore be assumed when assessing issues potentially requiring the use of the effects doctrine,[90] or any other principle diverging from strict territoriality.

### 2.3 Extraterritoriality

As it was with the previously discussed concepts, it is far from easy to clearly determine, what one exactly means when speaking about extraterritoriality.[91] According to the definition presented by the UN International Law Commission, extraterritorial jurisdiction means "an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the state in the absence of such regulation under international law."[92] In the light of the definition above, the differentiation between territorial and extraterritorial claims of jurisdiction can often be unclear, as assertions often incorporate both territorial and extraterritorial elements making the border between the two rather hazy.[93] Adding to the confusion, different meanings are given to extraterritoriality in different jurisdictions, with the US system focusing on state boundaries' role as limiters of how broadly a state

---

treat such agreements as unlawful, *it is safe to assume that Congress certainly did not intend the Act to cover them*." (*Alcoa*, p. 443) [emphasis added]).

[89] See, e.g., Mann 1973, p. 89–90, stating that from the point of view of international law, the court decisions where jurisdiction is based on the effects doctrine cannot be justified.

[90] Kuner 2015a, p. 239.

[91] Svantesson 2015a, p. 226.

[92] ILC 2006, p. 516.

Interestingly, historically, extraterritorial assertions were mostly caused not by states extending the territorial scope of their laws, but by states not being willing to assume jurisdiction over foreigners on their territory to states attempting to extend their jurisdiction well past their geographical borders. For example, according to Kassan, some elements of extraterritoriality can be found in the ancient world, even predating the Greek and Roman empires (Kassan 1935, p. 239–240, 247). It should be noted, though, that Kassan's argument of extraterritoriality originating in the ancient times is based on the fact that because back then (and, as noted in Bernhardt 1995, p 338, up until the Middle Ages), societies as whole were built around communities and not the geographical borders of a state, and the principle of territoriality as such was not recognised. Instead, the legislation was rather based on personality, i.e., the membership of a certain community. In such situations, a foreign person could not enjoy the rights and benefits of the local legislation and, consequently, was still extraterritorially subject to their own legal system. It was only after the enactment of the US Sherman Act (discussed above in note 85) when the attitude shifted towards the expansion of the territorial scopes of domestic laws.

[93] Svantesson 2015a, p. 227; Scott 2014a, p. 1343, 1345.

may exercise its jurisdiction, while the European approach differs in so far as state borders allocate jurisdiction to a certain party or parties, while withholding it from the others.[94]

In the absence of a clear definition, certain commentators have even gone as far as deciding to avoid using the term "extraterritoriality". According to Ryngaert, for instance, extraterritoriality should only refer to such assertions of jurisdiction that are made without any territorial link. As such cases are rare, a territorial link is therefore present, at least to a certain extent, in most so-called extraterritorial claims.[95] Additionally, it is pointed out that the term "extraterritoriality" often bears a certain negative connotation with people understanding extraterritorial assertions as automatically illegitimate or excessive.[96]

However, despite all the critique concerning the mere notion of extraterritoriality, for the purposes of this work, it is sufficient to assume a simple and rather broad definition, which vaguely resembles the ILC definition quoted above. According to the definition assumed here, extraterritoriality refers to the state's endeavour to control the activities of a person – natural or legal – situated outside its borders.[97] This definition captures the core meaning and purpose of extraterritorial assertions – the states' attempt to assert jurisdiction, control or affect events and conduct of persons originating or taking place entirely abroad, be it by means of legislation, adjudication, or enforcement. This definition does not make it possible to make a clear distinction between purely territorial

[94] Michaels 2006, p. 1058–1059.

[95] Ryngaert 2015b, p. 7–8. It should also be noted, though, that the mere concept of territoriality rests on the assumption that the physical location of persons, things and actions is knowable and known (for further discussion on this topic, see Eichensehr 2016, p. 145–146).

[96] Ryngaert 2015b, p. 8. Prompted by Ryngaert's findings, Kuner prefers to use the term "exorbitant jurisdiction" instead of "extraterritorial jurisdiction" (Kuner 2010b, p. 227). Buxbaum also finds that the terms "territoriality" and "extraterritoriality" are legal constructs that are often used with the intention to support or promote the user's personal interests (Buxbaum 2009, p. 635). However, as noted by Svantesson, and later acknowledged by Kuner, it is ultimately a factual and purely objective issue whether a claim of jurisdiction is "extraterritorial", but it is a subjective matter of opinion whether a claim is "exorbitant" – not all "extraterritorial" jurisdiction is necessarily "exorbitant" (Svantesson 2013b, p. 85; Kuner 2015a, p. 239).

[97] Svantesson 2015a, p. 227; Svantesson 2013b, p. 85. Svantesson formed this definition based on the definition of Senz & Charlesworth, according to whom extraterritorial jurisdiction is "the exercise of jurisdiction by a state over activities occurring outside its borders" (Senz & Charlesworth 2001, p. 72). Despite this definition being rather straightforward, it cannot be denied that in the modern interconnected world, it can be problematic to try to define the location of an activity, especially if it takes place in the cyberspace. For this reason, Svantesson proposes to define extraterritoriality through the location of the person engaging in the activity, instead of the location of the activity itself.

and extraterritorial claims; however, it is not its aim,[98] and it does not pose a problem for the purposes of this work. All claims of jurisdiction are to be treated and examined individually in their context in order to determine the extent of their extraterritoriality.[99] Additionally, the acceptability of a claim can neither be automatically tied to its extraterritoriality – whether a claim of jurisdiction is acceptable, should be decided only after assessing the claim as a whole, including the aims and the reasoning behind it.[100]

Using such a definition, it is very well possible to examine the extraterritorial extent of the European data protection law, which, after all, is the main aim of this work. As this definition is rather broad, many types of assertions will be seen as extraterritorial, at least to a certain extent. One further distinction can be made, however: there is a difference between what is meant by an "extraterritorial scope" (of, for instance, a certain legislative act), and what is meant by a mere "extraterritorial effect" (or impact).[101] The former refers to a direct extraterritorial assertion of jurisdiction that can be made by, e.g., formulating a legislative act in a certain way and by extending its territorial scope to directly cover certain conduct of persons situated abroad. Extraterritorial effects, on the other hand, can be caused by uses of jurisdiction that, despite being seemingly completely domestic and territorial, can still have an effect on international market.[102] For

[98] According to Svantesson, this definition instead makes it possible to determine whether an assertion of jurisdiction has any "extraterritorial effect or implications", further emphasizing that no mutually exclusive binary distinction can be made between territorial and extraterritorial claims (Svantesson 2013b, p. 85).

[99] Svantesson 2013b, p. 85.

[100] Svantesson 2015a, p. 227.

[101] Poullet 2007, p. 145. As with extraterritoriality as a whole, the distinction here is not binary either, as certain assertions may have an implicit extraterritorial scope. As it will be discussed later on, the importance of the differentiation between the extraterritorial scope and effect comes into play when assessing the extent and the severity of an extraterritorial assertion, and, therefore, its need for justification (see Svantesson 2015a, p. 227).

[102] See, e.g., C-366/10 – *Air Transport Association of America and Others*, where certain US airline companies claimed that the amendments introduced by the EU Directive 2008/101 were a unilateral attempt to extraterritorially impose the EU emission requirements on non-EU countries. The Court found, however, that the extraterritorial effects of the directive were acceptable as they were based on territoriality (or, as Scott frames it, the trigger for the application of the directive was territorial) – the requirements only applied to aircraft departing or arriving at airports within EU Member States (C-366/10 – *Air Transport Association of America and Others*, para 125–129; Scott 2014a, p. 1345). It cannot be denied, though, that despite its seeming territorial and domestic nature, the directive does have substantial effects beyond the borders of the EU (see also Coughlan et al. 2007, p. 33).

the purposes of this work, I will further expand the definition of extraterritoriality presented above to also include the incidental "extraterritorial effects" – influence on behaviour outside state borders, regardless of whether it is intended or not.[103]

Extraterritorial effects not explicitly integrated into the scope of a statute are especially often found in EU legislation.[104] It has been claimed that certain assertions extending beyond the borders of the Union are not "extraterritorial" as such, but rather employ a technique labelled "territorial extension". Territorial extension arises in cases where the application of a certain measure, such as a legislative act, is triggered territorially, but when certain circumstances abroad have to be taken into account when applying the measure.[105] According to Scott, an example of territorial extension is EU regulation 2111/2005, which regulates, *inter alia*, the access of aircraft to EU territory based on the aircrafts' global safety records.[106]

The EU's strict rules in relation to the consumer markets, combined with the Union's substantial market power,[107] causes another phenomenon that has been noted by Bradford – the "Brussels effect". The Brussels effect occurs when the EU uses its market power to influence activity abroad by the means of regulation that might initially appear completely domestic. It is, therefore, a matter of unilateral regulatory globalisation, which occurs when "a law of one jurisdiction migrates into another in the absence of the former actively imposing it or the latter willingly adopting it."[108] Such migration takes place in two stages. First, multinational companies adopt the EU standards adjusting their global activity to adhere to the EU requirements, resulting in a "*de facto* Brussels effect". Subsequently, often as a result of lobbying, the companies' local governments may adopt similar standards in their own jurisdictions in order to ensure equal opportunities for all companies on their market, which gives rise to "*de jure* Brussels effect".[109]

---

[103] See also Kuner 2015a, p. 236, arguing that it is not necessarily useful to even make a distinction between extraterritorial scope and effect.

[104] Poullet 2007, p. 148–149; Scott 2014b, p. 90 et seq.; see also Bradford 2012, p. 6.

[105] Scott 2014b, p. 90.

[106] Scott 2014a, p. 1343–1344.

[107] Bradford 2012, p. 11–12.

[108] Bradford 2012, p. 3–4. Bradford explicitly differentiates this kind of globalisation of standards from the one that is based on negotiated standards, or where certain requirements are imposed on other jurisdictions by the means of threats or sanctions.

[109] Bradford 2012, p. 6.

Bradford argues that the externalisation of EU regulation is a part of the so-called "race to top", where the economic development has triggered the enactment of increasingly strict regulation.[110] As a key prerequisite for the Brussels effect, Bradford highlights the geographically inelastic nature of consumer markets: as opposed to capital markets, the 500 million consumers residing within the EU are not likely to move location for regulatory reasons, causing the risk for non-compliant businesses to be left outside the whole European market.[111] Additionally, in order to be able to externalise its law, a state must have an established regulatory infrastructure and power over its large market, which is especially true in the case of EU and the regulation of data protection.[112] However, in the end, the success of the export of standards depends on the activity of the multinational companies – in order for a standard to become global, it must first be globally assumed by a company. For companies, it might often be economically sensible to adjust all global operations to adhere to the same standards, and, therefore, their role cannot be underestimated.[113]

Using the definition of extraterritoriality assumed above, it is evident that a rather wide array of different assertions can be considered extraterritorial, and that the Brussels effect has the potential to be one of them. Despite this, one could argue that when enacting legislation affecting multinational companies, the EU is not willingly trying to affect the companies' conduct outside the EU, let alone the regulatory activities of non-EU states, and that the global effect of the domestic regulatory activities of the EU is a mere accidental by-product of completely territorial legislation.[114] However, considering the definition described above, a mere incidental effect abroad – even if not intended – can constitute extraterritoriality. Therefore, influence on the conduct abroad caused by the Brussels effect should also be considered extraterritorial in spite of the legislation not being formulated with an explicit extraterritorial scope.[115] As unilateral regulatory

[110] Bradford 2012, p. 4–5.

[111] Bradford 2012, p. 16–17. As opposed to this, in a "race to bottom", a more mobile target, such as capital, can be moved to a jurisdiction with less strict regulation.

[112] Bach & Newman 2007, p. 835; Bradford 2012, 12, 22–23.

[113] Bradford 2012, p. 18 and 25; see also Drezner 2005, p. 845.

[114] Bradford 2012, p. 36 and 41 – the EU might argue that it merely enforces locally equal rules of the single market on both EU and non-EU companies with no attempt to extend the effect of its rules beyond the single market.

[115] It should also be considered that when enacting legislation, the EU is not unaware of its significant market position and the effects its legislation has on conduct abroad – as noted by Bradford, the EU does seek to "vigorously promote its interests on the global stage", and it has been criticized for attempting to practice a "novel form of imperialism" (Bradford 2012, p. 35–36). For an additional example of the EU's transnational regulatory action, see, e.g., Scott 2014a, p. 1363–1365, explaining

globalisation indeed does not require any active transnational coercive measures from the state enacting the legislation, the Brussels effect can be seen as one of the "mildest" versions of extraterritoriality.

It is clear that the definition of extraterritoriality assumed in this work is rather broad. However, it can be concluded that this definition focuses on the actual outcome of an assertion of jurisdiction – whether a state has actually attempted to control the activities of persons outside its borders – regardless of the means used in the attempt. Therefore, this definition constitutes a kind of a pragmatic approach to extraterritoriality, which will be applied in practice later when I will discuss in detail all the different extraterritorial dimensions of the GDPR.

### 2.4 Issues related to extraterritoriality

As indicated previously, independent states possess a specific set of rights that they are entitled to practice exclusively. This phenomenon is commonly referred to as sovereignty.[116] One of the most apparent grounds for critique of extraterritorial assertions of jurisdiction is that such assertions encroach on these prerogatives of other states.[117] Therefore, the problems related to extraterritoriality stem from the inherent nature of extraterritoriality as a concept: as a starting point, sovereign states should be able to fully regulate the conduct taking place on their territory – extraterritorial assertions by other states, however, contravene with this principle.

States often have divergent values that are reflected in their law. For instance, the United States clearly emphasises the importance of the freedom of speech above the right to privacy,[118] as it appears from its status as the First Amendment right and as supported by the US Supreme Court in, e.g., Bartnicki v. Vopper.[119] As opposed to this, the European Union is known for leading the way in the field of privacy regulation, with

---

the extraterritorial extent and the global effect of the EU capital market legislation and demonstrating the EU's readiness and willingness to directly regulate conduct taking place outside its borders.

[116] As discussed above in section 2.1, in the context of this research, the EU acts as the party making assertions of jurisdiction – for this reason, while the EU is not fully comparable to other sovereign states, these differences are not relevant for the purposes of this work.

[117] Perritt 2000, p. 892.

[118] Whitman 2004, p. 1209. As opposed to the EU, there is no single key federal act concerning data protection, and, instead, the regulation is fragmented by states and sectors (Petkova 2018, 1140).

[119] According to the US Supreme Court, "privacy concerns give way when balanced against the interest in publishing matters of public importance." (*Bartnicki v. Vopper,* p. 534; see also Wimmer 2018, p. 571).

privacy even being called the “Europe’s First Amendment”.[120] Therefore, when requiring US businesses to comply with EU data protection requirements,[121] the EU, in a sense, forces its values upon the US, despite the US having its own divergent values that it is fully entitled to adhere to in accordance with the principle of sovereign equality.[122] Additionally, such assertion can also be seen to imply that the values of the state asserting jurisdiction, in this case the EU, are more important than the values of other states, such as the US.[123]

For these reasons, before I begin the examination of the actual extraterritorial mechanisms of the GDPR, it is first useful to establish the framework that will be used when critically reviewing these mechanisms. In this section, I will discuss some of the issues often related to extraterritorial assertions, focusing specifically on their justification and enforcement. After this, I will review certain principles that can potentially be viewed as limitations to extraterritorial assertions.

### 2.4.1 Justification of extraterritorial assertions

As extraterritorial assertions of jurisdiction almost always interfere, at least to some extent, with the sovereign rights of other states, it is always necessary to properly justify each assertion. Often multiple states with intersecting ambitions may take interest in regulating a certain matter[124] – how should it be decided which state’s interests should prevail and which state should be able to assert jurisdiction over a matter? The second issue with extraterritoriality is, therefore, the range of difficulties surrounding the justification of an extraterritorial assertion.

First of all, it appears to be not entirely clear which party should be justifying an extraterritorial assertion. Some commentators view that the state asserting jurisdiction should itself validate the legitimacy of its assertion, whereas others claim that parties

---

[120] For further discussion concerning the differences between the difference of values between the US and the EU, see Petkova 2019. While the right to data protection is not absolute in the EU either (see, e.g., Recital 4 and Article 17(3)(a) of the Regulation and C-136/17 – *GC and Others*, para 57–59, 66), it is clear that the privacy is given a higher priority in the EU when compared to the US.

[121] For instance, pursuant to Article 3(2) GDPR, which will be discussed in section 3 below.

[122] Throughout this work, the US will often be used as an example of a target of extraterritorial assertions of the EU. While this is the case, the purpose of this work is not to provide insights that are only based on the EU–US relationship, but instead to evaluate the extraterritorial assertions made by the EU in relation to all non-EU states in general.

[123] See Svantesson 2013a, p. 278.

[124] For a general review of why states may choose to have an extraterritorial extent to their legislation, see ILC 2006, p. 516.

objecting to an assertion should name the rules of international law that are being broken by the contested assertion and, therefore, prove why the assertion is not legitimate.[125] It appears, though, that currently the common practice is that the party making an assertion should be the one proving its legitimacy, retaining the position of state sovereignty as a starting point in the assessment of extraterritorial claims.[126]

Above were discussed the traditional principles of asserting jurisdiction: the passive and active territoriality, the passive and active personality, and the protective and the universal principles and the effects doctrine. Especially the first six principles described in the Harvard Draft bear a sort of a deep-seated "acceptability value".[127] It has become clear, though, that reliance on the inherent acceptability of the principles is not sufficient in order to determine whether a jurisdictional claim is really legitimate.[128]

In the modern interconnected world, a single matter can have multiple independent regulators willing to claim jurisdiction based on different subjective interests, principles, and connections to the matter. Attempting to solve which state is entitled to claim jurisdiction over a case automatically based on the acceptability of the principle used would be unfair. One state might have a much stronger interest to assert jurisdiction based on, e.g., the interest to protect its nationals, as opposed to another state basing its jurisdiction on the more generally-accepted territorially. It does not help that with an increasing amount of activity taking place in cyberspace, the significance of geographical state boundaries is diminishing and the classical territorial principle starts to lose its meaning.[129]

---

[125] Lowe 2007, p. 179. It should be noted, though, there has never been a recorded instance of the latter situation with a state opposing an assertion demonstrating the existence of a rule prohibiting the assertion.

[126] Wimmer 2018, p. 559.

[127] Harvard Draft 1935, p. 445.

[128] See Wimmer 2018, p. 559.

[129] Svantesson 2015c provides an example: according to the territoriality principle, in cloud computing contexts, "state A always must have a jurisdictional claim over all aspects of data that happened to be located on a server located in state A". Considering the distributed transnational nature of cloud computing, with often numerous actions taking place simultaneously and multiple parallel copies of data being stored all in different parts of the world, it is apparent that a classical territorial approach is not practically applicable in this context. The difficulty of the situation was also highlighted in the Opinion of Advocate General Jääskinen in C-131/12 – *Google Spain and Google*, delivered on 25 June 2013, para 63, where the truly transnational nature of operations of Google Inc. and its subsidiaries was briefly described.

For these reasons, Svantesson has proposed a completely different approach to the question of justification of jurisdictional claims. He suggests that the principles for asserting jurisdiction described above, albeit well established, are outdated and actually part of the problem of justification[130] – according to his proposition, the classical principles as such should therefore be abandoned, as they are mere "proxy principles", and instead broken down to reveal the core principles contained within them. Consequently, jurisdiction should therefore be only exercised when the assertion meets the following three prerequisites:

1. The connection between the matter and the state willing to assert jurisdiction should be substantial;
2. The state willing to assert jurisdiction should have a legitimate interest in the matter; and
3. The assertion of jurisdiction should be reasonable considering the proportionality of interests of the state asserting jurisdiction and competing interests of other states, and, in some cases, other parties.[131]

This approach strongly reflects the broad individual approach to extraterritorial claims, as the three core principles listed above make it possible to individually assess all motivations and reasoning behind even the most controversial extraterritorial claims.[132] However, neither does this approach provide a succinct and straightforward solution to the problem of assessing the legitimacy of an extraterritorial assertion. What kind of a connection between the matter and the state is substantial enough? What kind of an interest is so legitimate that a state could assert jurisdiction based on it? Which types of interests can be considered more important than others, and why? With every controversial case requiring separate attention and assessment and with the absence of objective criteria for the assessment, Svantesson's approach does help one not to constrain their thinking with 80-year-old principles of Harvard Draft,[133] but still does not provide any much clearer guidelines for the actual assessment.

---

[130] See Svantesson 2015c, arguing that these principles were formed to reflect the legal practice at the time of the Harvard Draft, over 80 years ago. See also Mann 1973, p. 27–28, acknowledging the need to reconsider the principle of territorial jurisdiction for practical reasons even before the dawn of cyberage.

[131] Svantesson 2015a, p. 227; for further detail on how the proposed principles relate to the Harvard Draft, see Svantesson 2015–2016, p. 71–72.

[132] See, e.g., Svantesson 2015a, p. 227.

[133] Svantesson 2015–2016, p. 72.

Svantesson acknowledges the issue and counters by stating that although the proposed core principles do not provide a new easy way to automatically assess the legitimacy of an assertion, neither actually do the Harvard Draft principles. If one were to assess the allocation of jurisdiction over a transnational cloud arrangement[134] by means of classical principles of territoriality and personality, it would soon become clear that these old principles can hardly be applied to such novel circumstances. Therefore, even though the new principles do offer more space for interpretation, even more substantial difficulties arise when trying to apply the old principles less suited for the modern world.[135] For this reason, it is sensible to assume a more modern approach to the justification of extraterritorial claims – not by the means of the Harvard Draft principles, but by using the core ideas contained within them. Nevertheless, the Harvard Draft principles should not be abandoned completely – they still have utility when, e.g., examining the mechanisms of extraterritorial assertions and they can still be used as a part of the argumentation for or against the legitimacy of an assertion.[136]

### 2.4.2 Extraterritorial enforcement

As already discussed above in relation to the use of enforcement jurisdiction, the general international law does not allow for a state to perform such measures on the territory of another state, which only the state officials are entitled to perform.[137] Akehurst highlights that this condition applies even if certain individuals in the second state consent to the measures of the first state – the consent would then concern an encroachment of the state's sovereignty, which, in principle, cannot be consented to by any individual persons or entities.[138] If a state has no way to enforce the extraterritorial scope of its legislation, what is the objective of such assertion?

---

[134] See example above in note 129.

[135] Svantesson 2015–2016, p. 72. Svantesson also considers it possible that a set of new, more specific "proxy principles" can be developed based on the three core principles discussed above. If such principles can successfully facilitate the assessment of extraterritorial assertions while closely reflecting the values of the core principles, Svantesson welcomes them.

[136] The Harvard Draft principles can be used as a part of justification of an assertion especially when determining the extent of the connection between the state asserting jurisdiction and the subject matter. On the synthesis of the principles see also, e.g., Currie 2008, p. 352–354, suggesting that various principles could be applied considering, among other things, the circumstances of the matter and the interests of the states involved.

[137] Akehurst 1972–1973, p. 146; Currie 2008, p. 335–336; Kuner 2010b, p. 232; Ryngaert 2015b, p. 31; see also *The Case of SS Lotus,* para 45.

[138] Akehurst 1972–1973, p. 147. Akehurst notes that at times, states have consented to other states taking such measures on their territory, but, according to him, this does not alter the main rule that without a proper permission, such measures are against international law.

It has been argued that the real extraterritorial scope and effectiveness of a law is indeed measured not by how it is written, but how it is put into action, i.e., by the use of enforcement jurisdiction, as opposed to use of legislative jurisdiction.[139] Following the footsteps of renowned positivists Hart[140] and Kelsen[141], one could even go as far as arguing that the whole legitimacy of a law is compromised in situations where there is no real chance of enforcement of the said law.[142] Without assuming such a radical view, it still cannot be denied that a law does lose some of its meaning when there is no real chance of enforcing it – after all, fear of sanctions is one of the most important motivators for ensuring compliance with the law.[143] This has led certain commentators to conclude that while the actual enforcement of the law does not necessarily matter when assessing its effectiveness, it is its enforceability that is essential.[144]

However, sanctions and enforcement action are not the only reasons why people do comply with the law.[145] If so, is enforceability really essential in order for the extraterritorial assertions to have a purpose? Svantesson approaches the problem by making a distinction between the so-called "bark jurisdiction" and "bite jurisdiction", with all assertions of jurisdiction belonging to either of these groups depending, essentially, on whether there is a possibility of enforcing a jurisdictional claim.[146] In many cases, extraterritorial claims fall specifically in the category of "bark jurisdiction" – they are mere attempts to regulate a certain matter, without any realistic chance of being enforced.[147] Assertions falling into the category of "bark jurisdiction" have been widely criticised as

---

[139] Goldsmith 2000, p. 139.

[140] According to Hart 2012, p. 116, one of the two conditions necessary for the whole existence of a legal system is that valid rules of behaviour contained in the legal system "must be generally obeyed" – if a law cannot be enforced, it cannot be considered generally obeyed.

[141] Kelsen 2005, p. 41–42: "A norm is considered to be valid only on the condition that it belongs to a system of norms, to an order which, on the whole, is efficacious".

[142] Similar ideas have been expressed even earlier: according to Bentham and Austin, there is no legal obligation without a threat of punishment, or "the evil of a sanction", see Morrison 2016, p. 365–366.

[143] See Kuner 2015a, p. 244–245; Kuner 2010b, p. 236.

[144] Kohl 2007, p. 205.

[145] This has also been acknowledged by Kelsen, who understood that certain moral or religious motives can also affect the actions of people: "A man fulfils his legal duty to pay his debts very often not because he wishes to avoid the sanction provided by the law against an individual who does not pay his debts, but because … if he does not pay his debts, he will lose his credit." Kelsen also states that conduct based on other motives than fear of sanctions can also be a sign of an efficacious legal order. Kelsen also acknowledges the view of Ehrlich, according to whom much of human behaviour is motivated by other reasons than fear of punishment or compulsion (Kelsen 2005, p. 24–28).

[146] Svantesson 2013b, p. 68–69.

[147] As opposed to "bark jurisdiction", "bite jurisdiction" refers to assertions that are actually enforceable in practice (Svantesson 2015b, p. 556–557).

"regulatory overreaching" – a situation that occurs when the "rules are expressed so generally and non-discriminatingly that they apply *prima facie* to a large range of activities without having much of a realistic chance of being enforced."[148] In such cases, when the scope of the law is much broader than what can actually be enforced, the respect for the law, or even the legal system, may be undermined.[149]

However, enforceability is not everything – the moral justifiability and the public's perception of the law should also be considered, as they can affect the outcome of an exercise of "bark jurisdiction".[150] There may be reasons why a state would choose to enact a law that cannot be fully enforced abroad. For example, when enacting the Singapore Personal Data Protection Act 2012, the Ministry of Information, Communications and the Arts of Singapore openly acknowledged the difficulties of enforcing extraterritorial claims but identified the deterrent effect the extraterritorial claims may still have despite the lack of proper enforcement. Additionally, such a claim can demonstrate the effort to treat domestic and foreign subjects equally.[151]

When an unenforceable law is morally justifiable, the threshold for non-compliance can be somewhat high – as a starting point, companies prefer not to be publicly viewed as deliberate law-breakers, even though the law in question could never be enforced.[152] However, such potential effect of a morally justifiable law can be hindered by the requirements of the law being excessive. This has especially been identified as a risk in connection with the EU data protection law, known for its broadly formulated and materially strict extraterritorial requirements that will be discussed in section 3. Even as

[148] Bygrave 2000, p. 225, see also Moerel 2011a, p. 29.

[149] Kuner 2010b, p. 235; Hijmans 2016, p. 476. This can be especially true in the case of criminal law, see Coughlan et al. 2007, p. 50.

[150] Svantesson 2015b, p. 561–566; Svantesson 2013b, p. 70.

[151] MICA 2012; see also Svantesson 2015a, p. 233.

[152] Svantesson 2013b, p. 70–71; Kohl 2007, p. 208; see also WP 56, p. 15, stating that despite an EU judgment not being recognised and enforced abroad, "there exist examples that the foreign web site may nevertheless follow the judgement and adapt its data processing with a view to developing good business practice and to maintaining a good commercial image." Such an assumption is, naturally, not always correct, especially if there is little to no publicity attached to the non-compliance. As an example of such compliance, see the case of Yahoo! Inc.: in 2000, a French court ordered the US-based Yahoo! Inc. and its French subsidiary to prevent access to certain sites distributing Nazi artefacts – despite there being no possible risk of enforcement of such a court order in the US, Yahoo! Inc. complied with it as to not be viewed as deliberately breaking the law (*LICRA v. Yahoo!*; Kohl 2007, p. 201–207; Greze 2019, p. 112).

acknowledged by the EU officials themselves, the EU makes broad extraterritorial assertions but pursues the enforcement of only a fraction of them.[153] From the point of view of international law, this potential disproportion between the morally justified interests and the actual severity of the requirements causes a risk of non-Europeans viewing the GDPR in a negative light, which may end up in a complete loss of respect for the EU data protection regime abroad.[154]

One additional thing to consider is the intent of the state enacting the law. Svantesson makes one further distinction between "bark jurisdiction" and "failed bite jurisdiction": when making an extraterritorial claim, does the state acknowledge that it will not be possible to enforce it, and is it aware of the claim's actual ramifications? Or is the claim made without further considering its practical application? While the latter case might jeopardise the credibility of a legal system, the former type of claims can be interpreted as the state making the claim perceiving having the right to regulate a certain matter while accepting that the regulation cannot be enforced.[155]

It cannot be denied that the enforceability does further affirm a law's legitimacy – after all, it is the best way of ensuring the compliance with the law.[156] However, as it has been made clear, enforceability is not everything. The law can have an effect even without a real possibility of it being enforced abroad. In addition to mechanisms discussed above, an effect can also be achieved, for instance, by the means of the Brussels effect discussed above – as certain standards are in use within the EU market, they can slowly find their way abroad by means of regulatory migration, creating an effect abroad that does not require any coercion or enforcement. As it will be discussed below, the EU data protection law influences behaviour outside the EU through multiple such mechanisms.

---

[153] WP 225, p. 3: "Under EU law, everyone has a right to data protection. *In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU*, for instance where the data subject is a citizen or resident of an EU Member State" [emphasis added]. See also Svantesson 2015a, p. 232.

[154] Svantesson 2015a, p. 233–234. Such loss of respect can result in even further diminished compliance, which, due to the fact that the GDPR is not fully enforceable abroad against a non-compliant company (see section 4.3 below), further feeds the loss of respect, potentially causing a vicious cycle.

[155] Svantesson 2013b, p. 71.

[156] Kohl 2007, p. 205.

### 2.4.3 Potential limitations of extraterritoriality

In addition to – and, to some extent, based on – the justification and enforceability issues identified above, international law can be seen to set out[157] some limitations to how broadly extraterritorial assertions of jurisdiction can be exercised. The existence of limitations concerning the use of enforcement jurisdiction is accepted more or less universally.[158] Additionally, most states and authorities do recognise the existence of limitations to the use of legislative jurisdiction,[159] but the actual content of such limitations remains unclear.[160] For this reason, one cannot definitely claim, what kind of an extraterritorial assertion of legislative jurisdiction is acceptable, and what, on the contrary, is not legitimate.

When discussing the limitations to the extent of assertions of jurisdiction in each case, at the core of the question is the determination of appropriate allocation of regulatory authority between the states concerned, or, as Mills puts it, "which idea of justice … would be the most just to apply."[161] In order to answer this question and determine applicable law, numerous tests and doctrines have been developed – these can help trace the connection between the party asserting jurisdiction and the subject matter of a certain case.[162] However, such tests are not always applicable, or, as highlighted by Kuner,

---

[157] Due to the decentralised nature of international law and in the absence of any single regulatory instrument addressing the allocation of jurisdiction, no clearly defined written rules concerning the allocation of jurisdiction – especially legislative – have been formulated and universally accepted (Ryngaert 2015b, 29–30, 35–36; Currie 2008, p. 4–5; McConville & Chui 2017, p. 254).

[158] Brownlie 2008, p. 309; Mann 1973, p. 111–113, 121; Buxbaum 2009, p. 664; such a limitation was expressed in, e.g., *The Case of SS Lotus* (p. 18–19) described above: "the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State".

[159] See *Barcelona Traction, Light and Power Co, Ltd*, p. 105, where, according to the separate opinion of Judge Fitzmaurice, international law "postulate[s] the existence of limits – though in any given case it may be for the tribunal to indicate what these are for the purposes of that case; and … involve[s] for every State an obligation to exercise moderation and restraint as to the extent of the jurisdiction assumed by its courts in cases having a foreign element, and to avoid undue encroachment on a jurisdiction more properly appertaining to, or more appropriately exercisable by, another State." See also Mann 1973, p. 38; ILC 2006, p. 520; Ryngaert 2015a, p. 74–75; cf. Akehurst 1972–1973, p. 187, according to whom it appears that there are no limitations to the extraterritorial practice of legislative jurisdiction in the area of private law.

[160] Kuner 2010a, p. 185–186: Kuner notes that when states are willing to regulate a certain matter, they have been "creative" when coming up with justifications for their extraterritorial assertions of legislative jurisdiction.

[161] Mills 2009, p. 18.

[162] Kuner 2015a, p. 242. Kuner mentions, e.g., the test concerning the "centre of gravity" of a dispute or the determination of minimum connecting factors to the forum. Such tests often boil down to the core principles of comity and "jurisdictional reasonableness"

the use of such doctrines can even be attempted to be ruled out.[163] For instance, in relation to the EU data protection law, both the Advocate General Jääskinen and the Article 29 Working Party have emphasised the nature of the EU data protection regime as an independent system that is not subject to jurisdiction tests conducted under international law. Instead, according to these statements, only the system's own rules for determining jurisdiction should be applied.[164] While this is the case, principles of comity and sovereign equality still cannot be discarded – such a solution would be diplomatically unsustainable. Instead, these principles should be used to assess whether the EU's assertions of jurisdiction are reasonable.[165]

In addition to the uncertain existence and the uncertain applicability of the possible limiting principles, another challenge is posed by the subjective nature of the question. Instead of an objective assessment of which party should really be the one asserting jurisdiction based on the close connection and greatest interests involved, arguments concerning the legitimacy of an extraterritorial assertion are often based more strongly on the parties' subjective values.[166]

Despite these difficulties, certain solutions to the issue have been proposed and introduced in practice. In addition to the general and somewhat ambiguous international law principles of comity and "jurisdictional reasonableness", some more concrete solutions

---

[163] Kuner 2015a, p. 243.

[164] See the Opinion of Advocate General Jääskinen in C-131/12 – *Google Spain and Google*, delivered on 25 June 2013, para 54: "the interpretation of the Directive in accordance with the Charter *cannot add any new elements that might give rise to the territorial applicability of the national legislation implementing the Directive to those laid down in Article 4(1) of the Directive*. Article 8 of the Charter must, of course, be taken into account in the interpretation of the concepts used in Article 4(1) of the Directive, but the *points of attachment defined by the EU legislator cannot be supplemented with an entirely new criterion* by reference to that fundamental right" [emphasis added]. See also WP 56, p. 6: "As the directive addresses the issue of applicable law and establishes a criterion for determining the law on substance that should provide the solution to a case, the directive itself fulfils the role of a so-called "rule of conflict" and no recourse to other existing criteria of international private law is necessary."

Similar opinion has been expressed in connection with the autonomy of EU fundamental rights law: in C-402/05 P – *Kadi and Al Barakaat International Foundation v Council and Commission*, para 316, the Court stated that "the review by the Court of the validity of any Community measure in the light of fundamental rights must be considered to be the expression, in a community based on the rule of law, of a constitutional guarantee stemming from the EC Treaty as an autonomous legal system which is not to be prejudiced by an international agreement." The Court essentially highlighted the autonomous nature of certain principles of EU law and stated that they prevail over international law, referring to, in particular, provisions of international agreements (Hijmans 2016, p. 472–473, 505). See also Kuner 2014, p. 62 et seq. and C-584/10 P – *Commission and Others v Kadi.*

[165] If necessary, these principles can also be relied on in order to find alternative regulatory solutions that would be better in line with international law.

[166] Kuner 2015a, p. 241; see also Koskenniemi 2005 p. 513–515.

can be used in order to define the limits of one state's jurisdiction and, consequently, avoid potential conflicts. For instance, in the field of competition law, Ryngaert highlights the importance of different means of co-operation between the states, including reciprocity and communication, as a prerequisite for the avoidance of jurisdictional conflicts.[167] Kuner, on the other hand, proposes that the applicability of a law[168] should directly follow its enforceability – if there is no reasonable chance of the law being enforced, the assertion of legislative jurisdiction made in the scope of the law should be limited as well.[169] Such an approach, however, would be prone to strip the law of its other possible extraterritorial effects discussed above, which is why enforceability cannot be considered the only determining factor when assessing whether an extraterritorial assertion of legislative jurisdiction is truly legitimate.

Furthermore, Scott specifies two limiting instruments that already appear in the EU legislation. These instruments do not act as external restraints on extraterritorial assertions *per se*; instead, Scott characterises them as "safety valves" – principles that are built into the law to prevent the extraterritorial claims made by the law from mushrooming unreasonably. These principles are contingency and contextuality. As Scott describes them, contingency refers to situations where the EU, despite its increasing ambitions to regulate conduct taking place abroad, is also prepared to refrain from applying its legislation abroad in cases where it considers that the non-EU state has sufficiently regulated the matter itself, without requiring the use of strictly identical standards. As regards contextuality, it is used in order to reduce the rigidity of EU law and, on the contrary, to assess the applicability of EU law to a given case based on a nuanced contextual case-by-case review of a specific set of circumstances.[170] Scott indicates the use of both of these instruments in various extraterritorial EU laws that concern the regulation of financial market, but a similar dynamic can be observed in other fields of EU law, as

[167] Ryngaert 2015a, p. 64–65.
[168] In Kuner's example, data transfer regulations.
[169] Kuner 2015a, p. 244–245.
[170] Scott 2014a, p. 1365–1367.

well.[171] According to Scott, these instruments provide an opportunity for dialogue between the EU and third country regulators and reduce the one-sidedness of the extraterritorial assertions made in EU law. [172]

Based on the findings of this section, it can be concluded that there are no clear principles as to what kind of assertions are acceptable under international law, and what kind of assertions are exorbitant. Consequently, the assessment of the extraterritorial mechanisms of the GDPR should be carried out considering all relevant factors: the level of connection between the regulator and the matter, the interests of the regulators involved, their proportionality, predictability, fairness, and enforceability. However, before such assessment can be carried out, we will first examine research question (1) and look into the actual mechanisms of the GDPR that have an effect outside the EU borders.

# 3 Extraterritorial mechanisms of the GDPR

The enactment and the entry into force of the General Data Protection Regulation was, without a doubt, a great leap in the field of privacy regulation. In addition to the introduction of strict material requirements, a rather broad territorial scope was also adopted as part of the regulation. The territorial scope has since been subject to heated discussion and passionate critique by commentators worldwide. According to some views, the broad territorial scope of data protection legislation protects the rights and freedoms of individuals from threats caused by lax data protection requirements abroad.[173] On the other hand, broad cross-border data protection requirements are often viewed as an

[171] Contingency and contextuality, as described by Scott, do not appear in the EU data protection law. However, the adequacy decision system of the EU data protection law in the direction of contingency: according to the Article 45, personal data may be transferred to a third country if the European Commission has decided that the country is able to ensure an adequate level of protection of personal data. The European Commission does not require for the foreign data protection safeguards to be identical to those of the EU – instead, an adequacy decision is based on an overall assessment of, *inter alia*, relevant legislation, rule of law, respect for human rights, existence and functionality of supervisory authority, and other relevant factors (for an example of argumentation, see the recent Commission Implementing Decision (EU) 2019/419 concerning the adequate level of protection of personal data in Japan. The decision examines the system of Japanese data protection legislation and the rights and obligations contained therein in contrast to the EU data protection requirements). The nature of adequacy decisions and their effect outside the borders of the EU will be discussed in detail in section 3.3.1.

An adequacy decision does not make the GDPR not applicable to the processing abroad, as it should under Scott's description of contingency (Scott 2014a, p. 1366), but it still does achieve similar results: flexibility, openness to dialogue with third countries and diminished unilateralism.

[172] Scott 2014a, p. 1365.

[173] See, e.g. Reding 2012, p. 127.

unjustified encroachment on other states' domestic interests.[174] The latter view has gathered a lot of attention especially outside the EU: the territorial scope of EU data protection law has been called "an effort to impose the EU's will on the US" by US officials[175] and characterised as "aggressive".[176]

The Council of Europe Convention 108 acted as a basis for the Data Protection Directive, and, subsequently, the General Data Protection Regulation that replaced the Directive.[177] As argued by de Hert & Czerniawski, it allows for and even encourages the expansion of the territorial scope of the data protection legislation.[178] Respectively, the GDPR employs multiple different mechanisms of affecting data processing activities outside the EU. Some of these mechanisms are written directly into the text of the regulation, such as its broad territorial scope under Article 3 or the regulation of cross-border data transfers under Articles 44–50, whereas certain other effects are more discreet and not based on specific GDPR provisions, such as the Brussels effect of the GDPR.

## 3.1 General territorial scope of the GDPR (Article 3)

### 3.1.1 Operator's establishment within the EU (Paragraph 1)

Article 3 GDPR provides for the general territorial scope of the regulation. First paragraph of the Article concerns situations where personal data is processed in the context of the activities of an establishment of the controller or processor[179] within the EU. Paragraph 1 reads as follows:

---

[174] Kuner 2015a, p. 235–236; Bauchner 2000, p. 715.

[175] Cnet 2002.

[176] Goldsmith & Wu 2006, p. 175.

[177] The principles of Data Protection Directive were directly based on the principles of the Convention 108 (see COM(92) 422 final – SYN 287, p. 4–5). The same principles have then been incorporated and expanded in the General Data Protection Regulation. While the aim of this section is to look into the extraterritorial mechanisms of the GDPR, as certain provisions that will be reviewed here are similar in both the GDPR and the DPD, the interpretation of the DPD will also be given importance over the course of this work, where relevant.

[178] de Hert & Czerniawski 2016, p. 231–232. According to the updated Article 3(1) of the Convention, "Each Party undertakes to apply this Convention to data processing subject to its *jurisdiction*" [emphasis added], signifying a departure from the strict territorial approach.

[179] Under Article 4 GDPR, "controller" refers to a party that "determines the purposes and means of the processing of personal data". As opposed to the controller, "processor" refers to a party that "processes personal data on behalf of the controller". As in the context of the applicability of the GDPR it is mostly irrelevant whether a company acts as a controller or a processor, hereinafter controllers and processors will be jointly referred to as "operators".

> *"This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."*

This paragraph is similar to that of the Data Protection Directive, where, in Article 4(1)(a), a similar territorial scope concerning the "processing carried out in the context of the activities of an establishment of the controller on the territory of the Member State" was in place. The meaning and the true reach of the provision has caused a great deal of uncertainty[180] – what constitutes an establishment within the EU, and when is the processing considered to be carried out in the context of the activities of such establishment?[181]

#### 3.1.1.1 Evaluation of the establishment criterion and the relevant case law

At first sight, the nature of this Article 3(1) appears to be purely territorial – the GDPR is applicable when an operator established in the EU engages in data processing activities. However, this is not the case, as the provision does neither require that the establishment in the EU acts as an operator, nor that the processing activities should take place within the EU.[182] In the end, the provision applies to a surprisingly wide panoply of activities, which has been demonstrated in the CJEU case law. *Google Spain*[183] and *Weltimmo*[184] have established the broad territorial reach of Article 4(1)(a) of the Directive,[185] demonstrating that the Directive could apply to operators established outside the EU should they have a certain relevant establishment within the EU that could trigger the application of 4(1)(a). As the provision adopted in the GDPR is equivalent, this case-law sets significant precedents defining the future interpretation of the GDPR.[186]

---

[180] Svantesson 2016a, p. 210; Bygrave 2014, p. 199.

[181] Such twofold approach to the interpretation of Article 4(1)(a) of the Directive was adopted by both the CJEU (in relation to the Directive; see, e.g., C-230/14 – *Weltimmo*, para 28, 34) and the EDPB (in relation to the GDPR). However, when examining Article 3(1) GDPR, the EDPB raises an additional consideration considering the last phrase of the provision, further highlighting that the location of the actual processing activities plays no role in determination of applicability of the GDPR under Article 3(1) (see EDPB Guidelines 3/2018, p. 8–9).

[182] See, e.g., Moerel 2011b, p. 97; Van Alsenoy & Koekkoek 2015, p. 107.

[183] C-131/12 – *Google Spain and Google.*

[184] C-230/14 – *Weltimmo.*

[185] WP 179 update, p. 2.

[186] Svantesson 2016a, p. 210; Brkan 2016, p. 336.

In its judgment in *Google Spain*, mostly known for the CJEU confirming the existence of the right to be forgotten, the Court also addressed the interpretation of the phrase "in the context of the activities of an establishment [in the EU]" under Article 4(1)(a) of the Directive and its applicability to a non-EU operator with a subsidiary in the EU. The question before the Court was whether the processing activities carried out by the US-based Google Inc. could be subject to EU data protection law due to the fact that it was carried out for the purposes of advertising business activities of the Spain-based Google Spain SL. According to Google, the Spanish establishment had no role in the processing activities themselves and that the business of the Spanish establishment did not depend on the processing carried out by Google Inc.[187] CJEU found, however, that despite the processing activities taking place wholly within the US, these activities were still subject to the Directive under Article 4(1)(a) due to the fact that there was a significant economic link between the processing activities of Google Inc. and the advertising business of Google Spain SL.[188]

According to the CJEU, considering the business model of a search engine using advertising as its main source of revenue, the inextricable economic link between the activities constituted that "the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory."[189] Additionally, the Court renounced the restrictive interpretation of the Directive, referring to the general objective of the Directive to ensure the "effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data".[190] The Court also noted that the purpose of the broad territorial scope of the Directive was to prevent the circumvention of the Directive and the deprivation of natural persons of the protection guaranteed by the

[187] C-131/12 – *Google Spain and Google*, para 51; Van Alsenoy & Koekkoek 2015, p. 107.

[188] C-131/12 – *Google Spain and Google*, para 56.

[189] C-131/12 – *Google Spain and Google*, para 46, 56–57; despite the substantial differences in the conclusions concerning controllership and the existence of the right to be dereferenced between the Court and the Advocate General Jääskinen in *Google Spain*, the Court's views concerning the interpretation of Article 4(1)(a) of the Directive were similar to those expressed in the Opinion of Advocate General Jääskinen in C-131/12 – *Google Spain and Google*, delivered on 25 June 2013, para 64–68; see also WP 148, p. 10. The judgment has subsequently been criticised due to the fact that it remained somewhat unclear how the economic link should be interpreted in the context of differing business models (see Brkan 2016, p. 327).

[190] C-131/12 – *Google Spain and Google*, para 53. Here, the Court chose an approach focusing on the consequences of different possible interpretations, which it later referred to again in C-230/14 – *Weltimmo*, para 25 (see Svantesson 2016b, p. 335).

Directive.[191] A similar view concerning the restrictive interpretation of Article 3(a) GDPR was later adopted by the EDPB.[192]

Later, in *Weltimmo*, the CJEU further explained the content of Article 4(1)(a), especially focusing on the meaning of the notion of "establishment". The case concerned a Slovakian-registered company Weltimmo that ran a website for dealing Hungarian properties and provided the property advertisers with free trials of advertisement space on the website. Failing to delete the advertiser's data upon request, Weltimmo charged the advertisers for the services they did not want and, having not received payment, forwarded their data to debt collection agencies.[193] One of the questions before the Court was, in this case, whether Weltimmo has an establishment in Hungary, despite being registered in Slovakia, and whether Hungarian law was to be applied to the processing.[194]

The Court found that the only link Weltimmo had to Slovakia was the place of its registration – in all other respects, Weltimmo's business was connected to Hungary, where it had the customers, representatives, a bank account, and where it conducted the actual business and data processing activities.[195] When determining the actual place of establishment, the Court noted that "both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet."[196] In the end, the Court found that Weltimmo did have an establishment in Hungary, and that the processing of personal data was indeed carried out in the context of the activities of said establishment.[197]

---

[191] C-131/12 – *Google Spain and Google*, para 54.

[192] EDPB Guidelines 3/2018, p. 6.

[193] C-230/14 – *Weltimmo*, para 9.

[194] As noted by Advocate General Cruz Villalón, the role of Article 4(1)(a) of the Directive was dual, with the first role being the territorial extension of the applicability of the Directive to concern parties situated outside the EU processing personal data within the context of activities of an EU establishment (which was the case in *Google Spain*), and, on the other hand, to serve as a choice of law rule when determining, legislation of which Member State was to be applied to a certain case (Opinion of Advocate General Cruz Villalón in C-230/14 – *Weltimmo*, delivered on 25 June 2015, para. 23). With the introduction of the GDPR, it is evident that the significance of the latter role has greatly decreased, as, for the most part, the content of the Regulation is the same in all Member States (Brkan 2016, p. 336).

[195] C-230/14 – *Weltimmo*, para 32–33.

[196] C-230/14 – *Weltimmo*, para 29.

[197] C-230/14 – *Weltimmo*, para 38–39.

It has been noted that the criteria the CJEU used in *Weltimmo* when assessing whether the company had an establishment in Hungary bore a similarity with, and, in a sense, paved the way for the targeting test, which was later codified in Article 3(2) GDPR.[198] The Court rejected a formalist approach[199] and reflected the opinions expressed earlier in *Google Spain*, reiterating the fact that the concept of "establishment" should be interpreted broadly. By this, the Court lowered the threshold for "effective and stable arrangements" within a Member State[200] and further confirmed that Member State law – and, in the era of the GDPR, EU law – can be applicable even despite the operator's registered domicile not being inside the Member State, or the EU.[201]

The findings of *Google Spain* and *Weltimmo* were later adopted and reaffirmed in *Verein für Konsumenteninformation*[202] and *Wirtschaftsakademie*,[203] ascertaining the broad interpretation of Article 4(1)(a) in accordance with *Weltimmo* and *Google Spain*.[204] This subsequent case law further confirmed that "any real and effective activity, even a minimal one, exercised through stable arrangements" can constitute an establishment

[198] C-230/14 – *Weltimmo*, para 41; Svantesson 2016b, 337. The targeting approach will be discussed in further detail in the next section dealing with Article 3(2) GDPR.

[199] McCullagh 2016, p. 98.

[200] Revolidis 2017, p. 27.

[201] C-230/14 – *Weltimmo*, para 29–33, 39. Approach that was chosen in the *Weltimmo* judgment has been criticised: Revolidis, for instance, has argued that the broad concept of establishment creates an uncertain jurisdictional environment that maximises forum shopping and will authorise courts to adjudicate matters to which they have a trivial connection, undermining the quality of such decisions (Revolidis 2017, p. 27). Svantesson, on the other hand, has argued that the circumstances constituting the targeting in *Weltimmo* were highly straightforward and that such approach could be more difficult or even impossible to apply in more complex scenarios, questioning the utility of the targeting test (Svantesson 2016b, p. 337). However, here it is not necessary to further examine this critique, as it does not contribute to the general examination of the extraterritoriality of the EU data protection law.

[202] C-191/15 – *Verein für Konsumenteninformation*. *Verein für Konsumenteninformation* was a consumer protection case, which concerned the question of choice of law and the applicability of Rome I and Rome II regulations in an e-commerce setting. As the case concerned the intra-EU choice of law between the data protection laws of different Member States and introduced no significant new findings regarding the extraterritoriality of the EU data protection regime, the findings of the Court concerning the Rome I and Rome II regulations will not be discussed here in further detail; for a detailed analysis of the case, see, e.g., Law 2017.

[203] C-210/16 – *Wirtschaftsakademie Schleswig-Holstein*. Wirtschaftsakademie was a significant case in determining the allocation of controllership in the context of Facebook fan pages and cleared the fog around the interpretation of the concept of joint controllership (see, e.g., para 44).

[204] C-191/15 – *Verein für Konsumenteninformation*, para 73. Advocate General Saugmandsgaard Øe noted, however, that the broad interpretation in *Google Spain* was motivated by the aim to prevent the circumvention of the requirements of the directive – in *Verein für Konsumenteninformation*, on the other hand, the question concerned the choice between different Member State laws, which have both been drafted in accordance with the requirements of the Directive (Opinion of Advocate General Saugmandsgaard Øe in C-191/15 – *Verein für Konsumenteninformation*, delivered on 2 June 2016, para. 124–125). See also C-210/16 – *Wirtschaftsakademie Schleswig-Holstein*, para 54.

within the EU, and that Member State law (or, depending on the context, EU law in general) applies when processing takes place in the context of the activities of said establishment, even though the establishment itself does not engage in the processing.[205]

The EU case law has helped clear some of the confusion surrounding the interpretation of the establishment criteria. The findings were also later adopted by the EDPB, which has summed them up in relation to the interpretation of Article 3(1) GDPR and further emphasised the fact that according to the provision, the Regulation applies if all conditions of Article 3(1) are met "regardless of whether the processing takes place in the Union or not".[206] Considering the interpretations and the case law reviewed above, it is therefore evident that the territorial scope of Article 3(1) (and its counterpart in the Directive) is much broader than it may seem at first: as it was famously demonstrated in *Google Spain*, the California-based Google Inc. was considered subject to the requirements of the Directive. Next, however, I will examine the Article's next paragraph, the extraterritorial extent of which is somewhat more direct.

### 3.1.2 Data subjects situated within the EU (Paragraph 2)

Paragraph 2 concerns situations where the operator is situated abroad but processes the personal data of individuals within the EU. Paragraph 2 is, perhaps, the most explicit and clear manifestation of extraterritoriality in the EU data protection law – the provision attempts to directly regulate and have an impact on the conduct of operators outside the geographical borders of the EU with no establishment or any other kind of presence in the EU.[207] Paragraph 2 reads as follows:

> *"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

[205] C-191/15 – *Verein für Konsumenteninformation*, para 78, 80. In para 76, the Court did acknowledge, however, that there are limits to the broad interpretation of the concept of "establishment": the possibility to access an operator's website from a certain Member State, for instance, does not constitute an establishment in said Member State. See also C-210/16 – *Wirtschaftsakademie Schleswig-Holstein*, para 57, 60; de Lima Pinheiro 2018, p. 171.

[206] EDPB Guidelines 3/2018, p. 5–7.

[207] Azzi 2018, p. 127–128.

*(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

*(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."*

#### 3.1.2.1 Development of the provision

Article 3(2) has no similarly formulated counterpart in the Directive, but it can be seen as a kind of a successor of the Directive's Article 4(1)(c), under which Member State data protection law would be applicable to operators that process personal data making use of equipment situated within the Member State, regardless of the geographical location of the operator itself.[208] At the time of replacement, the provision was old and outdated, and there was a lack of clarity concerning its meaning.[209] Additionally, the "use of equipment" criterion was never clarified in CJEU case law, with questions concerning the interpretation of Article 4(1)(c) being dismissed in *Google Spain*[210] and *Rease and Wullems*[211] being withdrawn from the Court before a judgment could have been made.[212] However, it was made clear that the notion of "equipment" was intended to be interpreted broadly[213] and that the aim of the criterion was to further expand the territorial scope of the Directive to concern situations where an operator had no EU establishment and EU law could not be applied under Article 4(1)(a).[214] For this reason, Article 3(2) of the Regulation can be considered as a spiritual successor of Article 4(1)(c), since, as it will be discussed below, its aim is also to further extend the territorial scope beyond what has been established in relation to Article 3(1).

---

[208] According to the Article, Member State law was not applicable if the equipment in the EU was only used "for purposes of transit through the territory of the Community".

[209] It has also been noted that the ambiguity of the provision resulted in rather substantial variation in the national implementation of the provision, and thus a failure in harmonisation, further emphasising the need for a revision (Moerel 2011a, p. 29).

[210] Questions 1(b) and 1(c) to the Court concerned the interpretation of the "use of equipment" criterion under Article 4(1)(c). However, as the Court considered that EU law applied based on Article 4(1)(a), the Court saw no need to further examine Article 4(1)(c) (C-131/12 – *Google Spain and Google*, para 20 and 61).

[211] C-192/15 – *Rease and Wullems*.

[212] OJ C 78, 29.2.2016, p. 11.

[213] At the time of drafting, the provision was probably intended to concern large mainframe computers and other tangible equipment, whereas later is was expanded to concern non-physical technologies used in web browsing (Azzi 2018, p. 128). It has been debated, for instance, whether the use of cookies, JavaScript, ad banners or spyware constitutes "use of equipment" within the meaning of Article 4(1)(c) (see, e.g., Moerel 2011a, p. 29, 39–43).

[214] See, e.g., WP 179, p. 20.

As already noted above, the territorial scope provided for by Article 3(2) is rather broad, considering it affects all overseas operators' processing of personal data of EU data subjects that is related to the offering of goods and services to them or the monitoring of their behaviour in the EU. According to the original provision, along with recital 20, proposed in 2012, the regulation would have applied to *all* processing of personal data of data subjects residing in the EU, "where the processing activities are related to the offering of goods or services to such data subjects", or when monitoring of the behaviour of such data subjects is concerned.[215] The territorial scope of the original proposal was criticised for its vague nature and lack of further explanation of its meaning and the underlying principles,[216] especially considering the significance of a clearly defined territorial scope from the viewpoint non-European operators.[217]

As noted in the previous section, after the release of the 2012 proposal, a novel targeting criterion had begun to appear in some of the CJEU case law concerning the interpretation of Article 4(1)(a).[218] In 2014, in accordance with Advocate General Jääskinen's opinion, the Court found that the fact that a search engine "orientates" its activity towards the inhabitants of a Member State can be seen as a factor supporting the conclusion that the processing takes place "in the context of the activities of an establishment" of the operator within the EU.[219] In *Weltimmo*, the fact that a website that was "directed" at a Member State was considered as one of the factors that were to be taken into account when deciding whether an operator has an establishment in the targeted Member State.[220] The wider adaptation of targeting as a criterion for the applicability of EU data protection law without a proper provision allowing for it was

[215] COM(2012) 11 final, p. 20, 41. It should be emphasised at this point that the 2012 proposal did not include any limitations concerning whether an operator indeed intends to target the European market.

[216] See, e.g., Svantesson 2013b, p. 106, vividly describing the peculiar nature of the situation: "Anyone attempting to get clarification of the exact meaning of [Article 3] and the underlying principles that has guided the drafters, will logically turn to the Explanatory Memorandum [COM(2012) 11 final]. Unfortunately, doing so is an utter waste of time. Depending on one's personal disposition one will be either amused, dumbfounded or feel great despair in finding that under the heading '3.4 Detailed explanation of the proposal', all the Explanatory Memorandum states about Article 3 is the following: 'Article 3 determines the territorial scope of the Regulation.' If this is the 'detailed explanation of the proposal', we need the drafters to provide a 'super-extended director's cut' version as well." See also Tene & Wolf 2013, p. 6.

[217] Moerel 2011b, p. 92.

[218] The lack of a targeting criterion was one of the grounds for critique of the 2012 proposal, see Tene & Wolf 2013, p. 6–7.

[219] C-131/12 – *Google Spain and Google*, para 60; Opinion of Advocate General Jääskinen in C-131/12 – *Google Spain* and Google, delivered on 25 June 2013, para 68.

[220] C-230/14 – *Weltimmo*, para 41.

considered problematic,[221] but in the CJEU case law, targeting was always used as a mere auxiliary factor in order to confirm the applicability of the establishment criterion.[222]

The final version of Article 3(2), along with Recital 23, provided some additional level of clarity by officially adopting the targeting criterion.[223] Additional changes compared to the 2012 proposal are the narrowing of the scope to only concern people located in the EU instead of all EU residents worldwide,[224] addition of the clarification concerning the fact that a payment for goods or services is not required in order for the application of the GDPR to be triggered, and addition of the clarification that behaviour monitoring is subject to the GDPR only when the behaviour takes place within the EU.

#### 3.1.2.2 Evaluation of the targeting criterion and the relevant case law

As with the establishment criterion, when assessing whether individuals in the EU are targeted under Article 3(2), the EDPB recommends a two-step approach: first, it should be assessed whether the processing concerns data subjects within the EU, and second, it should be determined whether it indeed relates to the offering of goods or services or

---

[221] Brkan 2016, p. 328; see, e.g., suggestions in Moerel 2011a, p. 44.

[222] In *Weltimmo*, Advocate General Villalón stated that "Other factors, such as (…) the fact that the service provided by that data controller is directed at the territory of another Member State lack direct and decisive relevance for the purpose of establishing the applicable law, although these factors may constitute evidence of the real and effective nature of the activity for the purpose of determining the place of establishment and, in particular, when it comes to determining whether the data processing was carried out in the context of the activities of that establishment." Opinion of Advocate General Cruz Villalón in C-230/14 – *Weltimmo*, delivered on 25 June 2015, para 42. See also WP179, p. 31 and C-191/15 – *Verein für Konsumenteninformation*, para 34 (4b) and 72–81, where, despite the formulation of the question 4b, the Court did not comment on the directing of activities as a factor in the determination of applicable law.

[223] In recital 23, it was clarified which matters and circumstances should be taken into account when assessing whether an operator intends to offer goods or services within the EU. It was also acknowledged that "the mere accessibility of the controller's, processor's or an intermediary's website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention [to offer goods or services within the EU]" – the circumstances surrounding the activity should be evaluated as whole in order to define whether an operator really intends or "envisages" to do business on the EU market; see P7_TA(2014)0212, p. 5.

[224] Under the original proposal, under Article 3(2), the GDPR would have applied to processing related to data subjects "residing in the Union", which could have resulted in EU residents being entitled to rely on the protection granted by the GDPR even when travelling outside the EU. Under the current wording, the GDPR concerns the processing of personal data of all "data subjects who are in the Union", ruling out the possibility of applying the regulation to EU residents temporarily outside the EU. See Svantesson 2015a, p. 230.

Interestingly, the current Spanish and Portuguese wording of the paragraph still refers to individuals residing in the Union ("interesados que residan en la Unión" and "residentes no território da União"). Considering the explicit removal of the residence condition from the paragraph, in can be concluded that the GDPR indeed intents to refer to all individuals located in the Union, and not all individuals globally that have a place of residence in the Union (de Lima Pinheiro 2018, p. 2018).

to monitoring of their behaviour within the EU.[225] The first condition is quite unambiguous, despite the slight confusion concerning the fact whether one should reside in the EU for the GDPR to be applicable,[226] or if just a mere temporary location within the EU is sufficient to trigger the application of the GDPR. However, the confusion has been cleared in the enacted version of the Regulation, where it is made clear that just a mere location within the EU is sufficient in order to trigger the application of the GDPR in case all other conditions are met.[227]

The second condition is less clear: the operator providing the goods or services should be *targeting* individuals in the EU, or, as it is expressed in recital 23, it should be apparent that the operator "envisages offering services to data subjects" within the EU, in order for the GDPR to be applicable.[228] It is clear that the definition for "goods and services" is rather broad as it is explicitly stated that no payment is required for the processing to be subject to the GDPR.[229] However, the conditions for the fulfilment of the targeting criterion are less clear – as it appears from the case law reviewed below, the fulfilment of the condition requires the subjective intent of the operator to be observed.[230]

The recital 23 provides examples of factors which, on one hand, do not constitute the targeting of a Member State and which, on the other hand, "may make it apparent" that data subjects in a Member State are targeted. While it is acknowledged that, e.g., the

[225] EDPB Guidelines 3/2018, p. 11.

[226] Confusion was caused by the presence of the residence requirement in the Paragraph 3(2), when compared to recitals 2 and 12 of the same proposal claiming that data protection requirements of the GDPR should apply regardless of nationality of residence of natural persons. See, e.g., Svantesson 2013b, p. 107, basing his view on the Paragraph 3(2) 2012 proposal. Additionally, the targeting criterion was already included in the Recital 15 of the 2011 draft version of the GDPR Proposal, adding to the confusion when the criterion was removed (See Draft GDPR proposal 2011 (Version 56), p. 20; see also Kuner 2012, p. 6).

[227] See also EDPB Guidelines 3/2018, p. 13.

[228] This targeting test is familiar from the EU consumer protection law, see Svantesson 2015a, p. 231.

[229] The specification that no payment is required is rather significant in the context of data protection. Considering that many online services get their revenue from advertising, the data subjects, who do not pay to use the online service – along with their data – become a product from a commercial point of view, and the advertisers become the actual clients of such online service providers. However, while this is the case, the GDPR still applies due to the lack of the payment requirement.

[230] Svantesson 2015a, p. 232.

accessibility of the operator's website[231] or contact details or the use of a language generally used in the country where the operator is established does not ascertain the operators intention to offer services to data subjects in the EU, the use of specific Member States' languages or currencies or references to customers in the EU may mean that individuals in a Member State are targeted in accordance with Article 3(2).

In addition to the recital 23, when discussing the targeting criterion, the EDPB refers to the CJEU case law in joined cases *Pammer & Hotel Alpenhof*,[232] where the CJEU clarified the conditions for "directing activity to [a] Member State" under Brussels I regulation.[233] In *Pammer & Hotel Alpenhof*, the Court took a stand on the interpretation of the concept of "directing activities" within the meaning of Article 15(1)(c) of Regulation 44/2001, and, specifically, whether the accessibility of a website from a Member State justifies the conclusion that an activity is directed towards the said Member State.[234] The Court created an extensive but non-exhaustive list of matters that should be considered when ascertaining whether "it is apparent from [the trader's] websites and the trader's overall activity that the trader was envisaging doing business" with consumers in the EU, confirming that a mere accessibility of a website from a Member State does not constitute that activities are orientated to the said Member State.[235] The matters constituting evidence for the conclusion that a Member State is targeted include, *inter alia*, the international nature of the activity, the use and the possibility of making a reservation in the language of the targeted Member State, the use of international codes with telephone numbers and the use of a non-local top-level domain name.[236]

---

[231] Cf. C-191/15 – *Verein für Konsumenteninformation*, para 76, where the Court noted that the mere accessibility of an operator's website in a Member State does not constitute an establishment within the meaning of Article 4(1)(a) DPD in this Member State.

[232] C-585/08 – *Pammer and Hotel Alpenhof*.

[233] EDPB Guidelines 3/2018, p. 15; the same case law was referred to in the context of targeting in EU data protection law even before the release of the EDPB Guidelines 3/2018, see, e.g., Tene & Wolf 2013, p. 7; Kuner 2012, p. 6–7.

[234] C-585/08 – *Pammer and Hotel Alpenhof*, para 24 and 31.

[235] C-585/08 – *Pammer and Hotel Alpenhof*, para 94, 95. From the perspective of international law, if mere accessibility of a website in the Union constituted targeting, the territorial scope of EU law would have expanded unreasonably as essentially anyone administering a website online would have to comply with the EU standards.

[236] C-585/08 – *Pammer and Hotel Alpenhof*, para 93. For some reason, the Court did not consider the use of geolocation technologies emerging at the time of the judgment, for which it has been criticised: the use of geo-location technologies can clearly signal an intent to target – or specifically to not target – a certain market (Svantesson 2015a, p. 232).

The list of considerations provided by the Court in *Pammer & Hotel Alpenhof* and later affirmed in *Mühlleitner*[237] and *Emrek*[238] is significantly more extensive than its counterpart in recital 23 of the Regulation and provides a great deal of factors to be assessed when determining whether it is apparent that individuals in a Member State are targeted. The judgment in *Pammer & Hotel Alpenhof* also strongly highlighted the subjective nature of "directing activities",[239] and the Advocate General Trstenjak stated that the applicability of the targeting criterion requires an undertaking to actively endeavour to conclude contracts with consumers in the EU, and that it is essential that there is active conduct on the part of the undertaking in order to gain customers within the EU.[240]

The targeting criterion specified in recital 23 appears to only relates to Article 3(2)(a) concerning the offering of goods and services to data subjects in the EU, and no active targeting requirement is introduced in relation to the behaviour monitoring under Subparagraph (b). Considering the rather broad definition of monitoring assumed in the GDPR,[241] it would, however, be somewhat unreasonable to assume that every single type of monitoring action concerning data subjects located in a Member State would be subject to EU law, regardless of whether such action is intentional.[242] Additionally, according to the EDPB, the word "monitoring" used in the Regulation implies the purposeful intention of the controller to process behavioural data concerning a data subject's conduct in the EU.[243] For this reason, and in accordance with the interpretation of the EDPB, it should be concluded that a variation of the targeting requirement also concerns Subparagraph (b), signifying that the operator should actively intend to monitor data subjects in the EU. For this reason, as an example, an operator of a Chinese social media would not be subject to the GDPR only based on the fact that it monitors the online behaviour of its Chinese users, some of which happen to be travelling in the EU,

---

[237] C-190/11 – *Mühlleitner*, para 44.

[238] C-218/12 – *Emrek*, para 27.

[239] C-585/08 – *Pammer and Hotel Alpenhof*, para 75–76.

[240] Opinion of Advocate General Trstenjak in C-585/08 and C-144/09 – *Pammer and Hotel Alpenhof*, delivered on 18 May 2010, para 63.

[241] The broad definition of "monitoring" can be seen in Recital 24 of the GDPR, where it is seen to refer to all types of activity where "natural persons are tracked on the internet [and using other types of networks and technology]", in particular in order to analyse or predict their behaviour or to make decisions concerning them (EDPB Guidelines 3/2018, p. 17–18); see also Article 4(4) concerning the definition of the term "profiling" and opinions expressed in WP 251 rev. 01, p. 6–8.

[242] From the perspective of international law, such an interpretation implying that even incidental monitoring of behaviour taking place within the EU could lead to overly broad territorial scope of the EU data protection law, causing the Regulation to apply to processing which the EU has no interest in regulating.

[243] EDPB Guidelines 3/2018, p. 18.

if, otherwise, the operator only aims its services at the Chinese market. Therefore, in order for the GDPR to be applicable to a certain processing activity based on Article 3(2)(b), it should first be ascertained whether such processing is related to the monitoring of behaviour of data subjects in the EU, and, secondly, whether the operator really intends to monitor the data subjects in the EU.

The significance of the extraterritorial effect of both of the subparagraphs of Article 3(2) is further emphasised by the fact that under Article 27, all operators that are subject to the GDPR pursuant to Article 3(2) are obliged to designate a representative within the EU.[244] The requirement is not absolute, however, as no representative needs to be appointed if processing is occasional or if it does not include processing of special categories of personal data on a large scale.[245] Here, it is not sensible to further discuss the specific situations when a representative should be appointed;[246] however, the existence of the requirement further goes on to prove the potential impact of the extraterritorial effects of the Regulation.[247] The significance of the representative will be further highlighted below in section 4.3 when discussing the extraterritorial enforceability of the GDPR.

### 3.1.3 GDPR applicable by virtue of public international law (Paragraph 3)

The last paragraph of Article 3 reads as follows:

> *"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."*

This provision is equivalent to the one contained in Article 4(1)(b) of the Directive. Despite the intriguing reference to public international law, the actual effect of the provision is not substantial – as an example, Recital 25 clarifies that the provision applies to processing taking place in Member States' diplomatic missions or consular posts on the

[244] Despite the Article 3(2) GDPR being completely new, a similar requirement concerning the appointment of a representative in the EU was expressed in Article 4(2) of the Directive.

[245] See also Recital 80.

[246] For further information about the requirement and the exceptions to it, see EDPB 3/2018, p. 19–23.

[247] While the requirement under Article 27 does not have a separate effect on the territorial scope of the GDPR, it has significance when discussing the extraterritorial enforcement of the Regulation. In section 4.3, I will examine the impact of having a designated representative in the EU on the enforcement of DPA decisions against non-European operators, and I will look into the question of whether a designated representative can be held liable for the non-compliance of the designating operator.

territory of non-EU states.[248] As the allocation of jurisdiction in such cases is laid down in multinational conventions, and, due to its well-established nature, such exercise of jurisdiction is therefore rarely disputed, there is no practical need to further examine the extent and the effect of Article 3(3).

### 3.2 Regulation of international data transfers (Articles 44–50)

Chapter V (Articles 44–50) GDPR regulates the situations where personal data can be transferred outside the geographical borders of the EU. Serving as an additional safeguard to the territorial scope discussed above, the aim of the Chapter is to ensure that no personal data leaves the EU without proper protective measures in place. The chapter is opened by Article 44, which reads as follows:

> *"Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined."*

Articles 45–47 describe all of the possible means of basing a transfer of personal data outside the EU – these are the reliance on adequacy decisions and the use of appropriate safeguards, such as Binding Corporate Rules or Standard Contractual Clauses.[249] All of these means for transfer will not be discussed in detail here, as it is not relevant for the purposes of this work[250] – instead, I will focus on examining the

[248] The EDPB reminds that not all processing by such operators will be subject to the GDPR, as not all of it falls within the material scope of the GDPR contained in Article 2. Another example of when the GDPR can be applicable pursuant to Article 3(3) is the processing of personal data that takes place on vessels with flag state in the EU, which are, therefore, under the jurisdiction of the said Member State (EDPB Guidelines 3/2018, p. 19; see also WP 179, p. 17–18 and Svantesson 2014, p. 66).

[249] Additionally, Article 49 contains a list of exceptions to the main rule permitting data transfers in certain specific situations.

[250] For an extensive review of the adequacy decisions, as well as the appropriate safeguards that should be in place in the absence of an adequacy decision, see ICO Guide to the GDPR, p. 261–274.

impact of the data transfer regulation in general. As a similar regulatory mechanism was in use in the Directive, where Articles 25 and 26 concerned the international data transfers, interpretations and opinions concerning the Directive remain relevant when discussing the data transfer provisions of the Regulation.

As opposed to the territorial scope under Article 3 of the regulation, there is much less ambiguity as to what kind of transfers of personal data fall within the scope of the provisions in Chapter V, even though the international data transfers are not defined as such in Article 4 of the Regulation.[251] The requirements in Chapter V apply to all transfers, regardless of the roles of the operators taking part in the process as the data importer and the data exporter,[252] except for transfers where personal data only transits through a non-EU country and where no processing activities take place in said country.[253] On the other hand, there has been some notable unclarity concerning the relation of the data transfer regulation to the general territorial scope of the Regulation – in some respects, they overlap, and a non-EU operator could be subject to the requirements of the EU data protection law both pursuant to the GDPR's territorial scope, and due to additional safeguards used when exporting the personal data outside the EU.[254]

The ways, in which the regulation of international data transfers has an effect outside the EU, are somewhat more specific and flexible when compared to those of Article 3, which, essentially, just provides that all of the GDPR should be applied to a non-EU operator if all relevant criteria are met. On the contrary, when personal data is initially collected by an EU operator and subsequently transferred outside the Union by the said operator, the parties of the transfer should decide which safeguards will be used to ensure the compliance with the GDPR.[255] Each of the safeguards have a somewhat

---

[251] This issue (in the context of the Directive) has been acknowledged in C-101/01 – *Lindqvist*, para 56.

[252] It should be noted, however, that currently, if a data transfer is based on the Standard Contractual Clauses, a transfer between two processors is not possible as no Standard Contractual Clauses have been approved by the European Commission for such cases; see European Commission – Standard Contractual Clauses.

[253] Korpisaari et al. 2018, p. 393–394. The Court has looked into the definition of a transfer in its judgment in C-101/01 – *Lindqvist*, para 56–71, were the Court found that upload of personal data to a website that can potentially be accessed from outside the EU does not as such constitute a transfer of personal data.

[254] Kuner 2015a, p. 244. The implications of this overlap, dubbed by Kuner as a "belt and suspenders" approach, will be discussed in further detail below in section 4.3.2.

[255] Here, it is assumed that the transfer is made to a country, concerning which the European Commission has not given an adequacy decision. The function and effect of the European Commission's adequacy decisions in the international community will be discussed in the next section.

different effect on the data importer located outside the EU: when using Standard Contractual Clauses, for instance, the importer binds itself to the enforceable data transfer agreement, the requirements of which are similar to those of the GDPR.[256] Or, when making an intra-group transfer of personal data, the data importer can undertake to comply with the Binding Corporate Rules approved by a national supervisory authority.[257] Other appropriate safeguards that can be used are, e.g., the use of approved codes of conduct or certification mechanisms together with enforceable commitments of the data importer.[258]

As described above, it is evident that when regulating international data transfers, the wording of the GDPR goes further than just to make an assertion of jurisdiction over the data importers – at the core of the permitted safeguards is their enforceability. Along with the requirement to use a data processing agreement when a transfer between a controller and a processor takes place,[259] these safeguards guarantee the EU a better control over the personal data leaving its territory. EU's control is, however, hindered by the fact that these safeguards rarely provide a level of protection identical to that of the GDPR[260] – in the light of the Snowden revelations, it has been challenged whether the Standard Contractual Clauses adopted by the European Commission years prior to the revelations are still able to provide an adequate level of protection to personal data exported from the EU to the US.[261] It is therefore evident that when regulating international data transfers, the EU is balancing between guaranteeing the adequate level of standards on one hand, and making them acceptable, enforceable and easy to comply with on the other. Such balancing is especially visible in the context of multilateral negotiations concerning level of data protection, which will be examined next.

---

[256] All current Standard Contractual Clauses are based on the Directive, as they have not been updated for the GDPR (ICO Guide to the GDPR, p. 266–267).

[257] ICO Guide to the GDPR, p. 265–266. The enforceability of the Binding Corporate Rules is highlighted in the Article 47(1) GDPR.

[258] ICO Guide to the GDPR, p. 268–269. There are, additionally, certain exceptional situations where additional safeguards need not be used. Conditions for such situations are listed in Article 49, and the EDPB has confirmed that they are to be interpreted restrictively (see EDPB-EDPS 2019, p. 1).

[259] For the requirements concerning the content of the data processing agreement, see, e.g., Article 28 GDPR.

[260] See, e.g., C-362/14 – *Schrems*, para 73

[261] The validity of, and the adequacy of the protection provided by the Standard Contractual Clauses, along with the Privacy Shield framework, have been questioned in CJEU Case C-311/18 – *Facebook Ireland and Schrems*, which will be discussed in further detail below.

## 3.3 Effects caused by regulatory globalisation

### 3.3.1 Regulatory globalisation through multilateral treaties and adequacy decisions

In addition to the direct cross-border effects of the GDPR provisions discussed above, there are certain more discreet ways in which the European data protection law affects the data processing activities outside the EU. First of all, when discussing the influence of the European data protection law, one cannot disregard the effect of the Convention 108. Although Convention 108 is a multilateral treaty of the Council of Europe, and not an EU legislative instrument *per se*, it has served as a basis for the development of the European data protection law.[262] Subsequently, certain non-EU countries have also joined and ratified the Convention 108 leading to the spread of data protection standards based on Convention 108 outside the European borders.[263]

Nowadays, it is argued that the EU has taken over the role initially assumed by the Council of Europe as the forerunner in the field of data protection.[264] With the Convention 108 undergoing modernisation, the Council of the European Union has found in its decision concerning the authorisation to ratify the updated Convention that due to the fact that the safeguards contained in both updated Convention 108 and GDPR are based on the same principles, the entry into force of the modernised Convention would result in, among other things, the further promotion and the raised awareness of the EU data protection standards at a global level.[265] Therefore, from serving as a basis for the EU data protection law, the EU now views Convention 108 as an instrument that can be used to export its data protection standards to an even broader range of non-EU countries.[266]

---

[262] Hustinx 2013, p. 9. Additionally, the influence of the OECD Privacy Guidelines (1980) cannot be denied, as the principles formed initially therein bear a similarity with the ones in the Convention 108. The influence of the Guidelines has been noticeable especially outside Europe until 1995, when the DPD providing for a higher level of data protection standards was adopted (Greenleaf 2019, p. 3–5). It should also be noted that while both the EU and the US are members of the OECD and subscribe to the Guidelines, the differences in the level of data protection between the two is substantial (Hijmans 2016, p. 456). It should also be noted that the Guidelines are not binding, as opposed to the Convention 108 (Bu-Pasha 2017, p. 1–2).

[263] Currently, Convention 108 has been signed and ratified by 8 Non-Members of the Council of Europe, including Argentina, Mexico, Uruguay and Senegal (see Council of Europe 2019).

[264] Hustinx 2013, p. 50.

[265] Council Decision 2019/682.

[266] However, the EU also allows for derogations based on international agreements: under Article 48, third country judgments or decisions requiring the disclosure of personal information may be recognised or enforceable only if there is an international agreement, such as a mutual legal assistance treaty, in force between the Member State and the third country requesting disclosure.

Another matter that the Council of the European Union found in the same decision was that the ratification of the updated convention would "facilitate data flows between the Union and the non-Union Parties to Convention 108", i.e., the ratification could streamline the process of international data transfers described in previous section. Such facilitation would be achieved, most likely, by the means of an increased amount adequacy decisions concerning those countries that have adopted the data protection standards of Convention 108 and implemented them in their national legislation.[267]

Adequacy decisions, as a starting point, permit data transfers from the EU to certain approved non-EU countries without any of the additional safeguards listed in Article 46 in place.[268] The decisions are made by the European Commission, and, therefore, are not bilateral treaties between the EU and the target state – however, the negotiation and preparation work in order for a state to achieve an adequate level of data protection involves cooperation between the target state and the EU.[269] Adequacy decisions are granted somewhat rarely: as of September 2019, only 9 countries and territories were given a full finding of adequacy.[270] From the perspective of the EU, the intent of which is to regulate all global processing of personal data relating to persons located within the EU, there is a notable drawback of the adequacy decisions and multilateral agreements concerning the level of data protection. As adequacy decisions, and especially the multilateral agreements, are prepared in cooperation between the parties,[271] the

[267] An example of this trend is the adequacy decision concerning Uruguay: at the 1118th meeting of the Ministers' Deputies of the Council of Europe in July 2011, Uruguay was invited to accede the Convention 108 (Dec(2011)1118/10.3). In August 2012, the European Commission gave a decision concerning the adequate level of data protection in Uruguay, in the reasoning of which it referred to, among other things, Uruguay joining the Convention 108 (Commission Implementing Decision 2012/484/EU, Recital 13). Accession to Convention 108 was also viewed as a favourable factor in the negotiations concerning EU-US Safe Harbour revision following the Snowden revelations in 2013, see COM(2013) 846 final, p. 9.

[268] ICO Guide to the GDPR, p. 263–264.

[269] For a glimpse of the process surrounding the adequacy negotiations concerning Japan and South Korea, see, e.g., Greenleaf 2018.

[270] Full findings concern Andorra, Argentina, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay, with only certain types of processing being covered by the adequacy findings of Japan and Canada, and with the US being considered adequate only under the EU-US Privacy Shield framework (European Commission – Adequacy decisions, see also ICO Guide to the GDPR, p. 264).

[271] It should be noted, however, that the internal guidelines used by the European Commission when carrying out an adequacy assessment have never been made public (Kuner 2017, p. 900–901).

achieved end result may not always be ideal from the EU's point of view, as some trade-offs may need to be made in terms of detailed requirements.[272]

### 3.3.2 Specific considerations concerning the EU–US relationship

A notable example of the compromises involved in bilateral cooperation were the negotiations between the EU and the US that eventually led to the adoption of the Safe Harbour Privacy Principles. While the US was reluctant to incorporate the EU privacy standards in its own legislation,[273] the Safe Harbour framework was negotiated between the EU and the US to facilitate the transatlantic flows of personal data. The EU mandated that the framework be put in place as the general level of data protection in the US did not meet the EU's requirements.[274] In accordance with the Commission Decision of 26 July 2000, operators certified under the US-EU Safe Harbour framework and complying with all secondary requirements set out in the decision were considered to provide an adequate level of data protection under Article 25 of the Directive.[275]

However, as the framework was a result of negotiations between the EU and the US, it did not perfectly reflect all of the EU's data protection standards. For instance, in the principles themselves it was stated that "Adherence to these Principles may be limited (…) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization".[276]

As expected, the Safe Harbour arrangement was vehemently criticised from the moment it was passed, as the framework did not meet the EU data protection requirements nor, e.g., the OECD Privacy Guidelines.[277] The wording of the principles was very vague,

---

[272] Gady 2014, p. 17. Interestingly, the possibility of compromise was initially denied be the advisor of the European Commission, Spiros Simitis, who argued that data protection "is not a subject you can bargain about", see Cate 1995, p. 439.

[273] Petkova 2018, p. 1141, 1143

[274] Weber 2013, p. 125.

[275] Commission Decision 2000/520/EC.

[276] Additionally, in Annex II, FAQ 2, it was clarified that where "the rights of a free press embodied in the First Amendment of the U.S. Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations." Furthermore, in Annex IV, Section B, it was acknowledged that the US organisations must prioritise the compliance with US law above the compliance with the Safe Harbour principles, and, in the case of a conflicting authorisation, respect must be paid to the "legislative prerogatives" of the elected lawmakers of the US. See also Petkova 2018, p. 1141–1142.

[277] See, e.g., WP32, p. 4–6.

leaving lots of room for interpretation and even "light" compliance being considered sufficient. The exceptions from the principles were rather broad, the efficiency of the self-certification mechanism at the core of the framework was questionable, and the compliance with the principles turned out to be inadequate.[278] These concerns were further amplified at the time of the Snowden revelations when the general public became aware of the US' large-scale data collection programs. Essentially, it was understood that the personal data transferred from the EU to the US under the Safe Harbour framework was not safe from US intelligence agencies, prompting the European Commission to commence work on the revision of the framework.[279]

Before anything was done, however, the whole Safe Harbour agreement was invalidated by the CJEU in *Schrems.*[280] The case before the CJEU originated from a complaint lodged in June 2013 in the wake of the Snowden revelations by Maximillian Schrems to the Data Protection Commissioner, the Irish DPA. The complaint concerned the EU–US data transfer practices of Facebook, and, in particular, the fact that US National Security Agency was intercepting Facebook's transfers of personal data from the EU to the US.[281] In his complaint, Schrems claimed that "the law and practice in force in [the US] did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities".[282] The case was first rejected by the Commissioner as unfounded, but the Irish High Court found that the mass surveillance carried out in the US undermined the security of personal data transferred to the US and that the Safe Harbour decision is not compliant with the requirements of Articles 7 and 8 of the EU Charter of Fundamental Rights.[283]

The CJEU found that the level of protection provided by the Safe Harbour framework was insufficient: while, according to the Court, the notion of "adequacy" did not require the level of protection to be identical to that in the EU, it should be "essentially equivalent

[278] Weber 2013, p. 126–127, Petkova 2018, p. 1142.

[279] COM(2013) 847 final, see, in particular, p. 16–18.

[280] C-362/14 – *Schrems*, para 107. Another of the Court's findings affirmed the national Data Protection Authorities' right and ability to question the adequacy decisions of the European Commission (para 66). Kuner argues that such one-sided examination of foreign law carried out by the Data Protection Authorities, and, ultimately, the CJEU, can, at worst, lead to "false application of foreign law" leading to conclusions far from the objective truth (Kuner 2017, p. 901).

[281] Lam 2017, p. 4.

[282] C-362/14 – *Schrems*, para 28.

[283] C-362/14 – *Schrems*, para 29–34.

to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter"[284] – the Safe Harbour framework, however, failed to guarantee such protection.[285] Additionally, the CJEU found that while the self-certification system as such was not flawed, the credibility of the whole framework was weakened considering the broad derogations in place, and due to the fact that the framework was only limited to commercial organisations receiving the personal data and that their compliance was in no way monitored.[286] The Court therefore acknowledged that while certain less significant trade-offs may be accepted when assessing the adequacy of data protection abroad, these trade-offs may not concern the core data protection requirements. This approach further demonstrated the EU's ambition and the main target of the EU data protection regime to provide protection for the personal data of data subjects in the EU transcending the borders of the Union, as, understandably, lax requirements outside the EU could undermine the whole purpose of the regime.[287]

The abrupt annulment of the Safe Harbour framework resulted in a great stir in different stakeholders ranging from EU and US government officials and academics to operators relying on the framework in EU–US data transfers.[288] The invalidation decision came into force with no transition period and the operators relying on Safe Harbour had to adjust their business practices quickly. Only a year later, in July 2016, the European Commission issued an implementing decision establishing and confirming the adequate level of data protection provided by the Safe Harbour's replacement, the EU–US Privacy Shield framework.[289] Structurally, the Privacy Shield framework is similar to the Safe Harbour,[290] as both are based on self-certification and adherence to a set of basic principles based on the EU data protection law, albeit more detailed than the ones in Safe Harbour. As opposed to the Safe Harbour, the Privacy Shield also includes obligations

[284] C-362/14 – *Schrems*, para 73; for further analysis of the meaning of term "adequate" in this context, see Opinion of Advocate General Bot in C-362/14 – *Schrems*, delivered on 23 September 2015, para 142.

[285] This restrictive interpretation of "adequacy" has been criticised, as it does not consider different cultural values affecting the level of data protection in different countries and as it places an increased burden on these countries if they wish to have a level of data protection that is considered "adequate", see Kuner 2017, p. 900–901.

[286] C-362/14 – *Schrems*, para 81–87.

[287] See, e.g., Poullet 2007, p. 144.

[288] Kuner 2017, p. 882–883.

[289] Commission Implementing Decision (EU) 2016/1250.

[290] Petkova 2018, p. 1153–1154.

for the US national security and intelligence agencies concerning the protection of personal data transferred to the US under the framework.[291]

However, despite the seeming improvements, the future of the Privacy Shield has also been questioned even before it came into force. For instance, the EDPS stated that "robust improvements are needed" for the framework to be solid and stable in the long term,[292] and the WP29 has expressed its concern in relation to, *inter alia*, the framework's lack of rules concerning data retention limitation, the continuously vague exemptions from the principles under Annex II, Section I.5. of the Decision 2016/1250, and the possibility of the collection of massive and indiscriminate data.[293] Certain reasons for insecurity originate from the US, as well: certain US legislative instruments are crucial for the Privacy Shield to function as intended[294] – however, these orders, issued before the Trump administration, form derogations from the US Constitution, and President Trump has threatened to repeal them.[295]

Despite the built-in annual re-evaluation mechanism, the future of the Privacy Shield is by no means certain.[296] As the framework was drafted under the Directive, it is unclear whether it truly offers an "adequate" and "essentially equivalent" level of protection under the much more complex requirements of the GDPR.[297] Some conclusion to this debate will arrive, however, once the CJEU gives its judgment in *Facebook Ireland and Schrems*,[298] which was heard before the Court in July 2019. Although the subject matter of the case is not primarily related to the Privacy Shield framework, its status has also

---

[291] See, e.g., Annex VI to the Commission Implementing Decision (EU) 2016/1250; WP 238, p. 4; Kuner 2017, p. 902–903.

[292] EDPS Opinion 4/2016, p. 12. It is clear from the comment of the EDPS that while future improvements are essential for the framework to be viable in the long run, the introduction of a framework as quickly as possible regardless of its possible shortcomings was important in order to greatly facilitate the EU-US data flows.

[293] WP 238, p. 17, 40.

[294] These instruments are the EO 12333 and PPD-28, see recitals 68–69 of the Decision 2016/1250.

[295] At his campaign rally in Greenville, NC, Trump proclaimed that "The change will begin my first day in office – number one, we're going to eliminate every unconstitutional executive order and restore the rule of law to our land", after which the discussion took a quick turn towards the construction of the US–Mexico border wall (C-Span 2016, at 6 minutes and 48 seconds). Both of these promises, however, are yet to materialise.

[296] For example, see the report on the second annual review that took place in late 2018, where the European Commission concluded that the US continues to ensure an adequate level of protection as regards personal data transferred to the US under the Privacy Shield framework but reminded the US to appoint the Privacy Shield Ombudsperson by 28 February 2019 (COM(2018) 860 final, p. 5–6). The US Senate appointed Keith Krach as the Ombudsman on 20 June 2019 (US Congress 2019).

[297] Kuner 2017, p. 903–904; Bu-Pasha 2017, p. 13–14.

[298] C-311/18 – *Facebook Ireland and Schrems.*

been contested in the reference for a preliminary ruling.[299] According to the Irish High Court, referring the matter to the CJEU, "Neither the introduction of the Privacy Shield Ombudsperson mechanism nor the provisions of Article 4 of the [decisions concerning the Standard Contractual Clauses][300] eliminate the well-founded concerns raised by the [Irish Data Protection Commissioner] in relation to the adequacy of the protection afforded to EU data subjects whose personal data are wrongfully interfered with by the intelligence services of the United States once their personal data have been transferred for processing to the United States."[301]

It is clear that uninterrupted data flow between the EU and the US are of utmost importance for the functioning of global economy. The balancing between ensuring the data flows and guaranteeing an adequate level of protection is not an easy task, especially now that the future of the Standard Contractual Clauses is also at stake – their annulment would affect all data transfers from the EU based on them, regardless of the destination country. It has been suggested that due to the nature of governmental data collection in the US, the CJEU could introduce new limitations to the Privacy Shield and Standard Contractual Clauses based data transfers to the US. On the other hand, the US is not the only non-EU country practicing indiscriminate data collection: for instance, Russian and Chinese data collection practices are neither compatible with the GDPR, but there are no additional limitations or safeguards to the Standard Contractual Clauses put in place for these states.[302] Therefore, it remains to be seen which interests will be prioritised by the CJEU.

### 3.3.3 Unilateral regulatory globalisation (the Brussels Effect)

Another means of affecting foreign operators' activities taking place outside the EU, and, in some cases, even the decisions of non-EU legislators, is by the means of unilateral

[299] The status of the Privacy Shield framework was directly challenged in T-738/16 – *La Quadrature du Net and Others v Commission* due to, *inter alia*, the collection of personal data by US authorities and the Privacy Shield framework not providing sufficient safeguards against such data collection, thus not ensuring an adequate level of protection. For these reasons, the applicants directly claimed that the Court should declare Commission Implementing Decision concerning the adequacy of the Privacy Shield Framework be contrary to Articles 7, 8 and 47 of the Charter and to annul the decision, which would exactly follow the CJEU's findings in *Schrems*. The hearings in the case were suspended until a judgment is issued in *Facebook Ireland and Schrems* (See Baker 2019a).

[300] In particular, this referred to the Commission Decision 2010/87/EU, as amended by Commission Implementing Decision (EU) 2016/2297.

[301] *The Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems*, para 339. The US legislation serving as a basis for the data collection was examined in, e.g., para 164–183 of the judgment.

[302] Swire 2019, Baker 2019b.

regulatory globalisation, also dubbed as the “Brussels effect”, which has already been discussed on a general level in section 2.3. As noted above, the Brussels effect occurs when, due to the substantial market power of the European Union, an activity outside the EU is influenced by EU law despite no direct attempt to achieve such an effect being made in the law – instead, such situations revolve around non-EU states and, more importantly, operators within these states voluntarily accepting and adopting the EU requirements and applying them to their own activity.[303] Brussels effect is, therefore, a type of regulatory globalisation where no coercion is exercised by the EU in order to make its standards adopted abroad.[304]

It is said that the Brussels effect caused by the GDPR is tightly linked to the data transfer regulation and the “adequacy-based framework” under Chapter V.[305] However, that is not necessarily always the case – Bradford argues that the Brussels effect should be separated from the politically negotiated globalisation of regulatory standards.[306] Despite the European Commission’s adequacy decisions being made unilaterally by the European Commission alone, they are prepared in cooperation with the target states and therefore do not satisfy the criteria for Brussels effect. As argued by Bradford, one of the key factors for the Brussels effect to occur is the activity of the operators: the effect is visible when a company operating in the European market implements a single set of standards based on EU law requirements to concern all of its global activity.[307] For this reason, the Brussels effect is related to both the data transfer regulation and the general territorial scope of the GDPR: once the European data protection standards apply to a part of the operator’s data processing activities, regardless of whether compliance is based on, e.g., Article 3, Standard Contractual Clauses, Binding Corporate Rules or the Privacy Shield framework, it can be easier for a foreign operator to adjust all of its processing activities to comply with the same set of requirements.[308]

---

[303] Bradford 2012, p. 11–12.

[304] Bradford 2012, p. 4.

[305] Lynskey 2015, p. 42–43.

[306] Bradford 2012, p. 4.

[307] Bradford 2012, p. 18 and 25.

[308] For actual examples of companies implementing certain EU data protection requirements globally, see the Facebook 2018 and Microsoft 2018.

Certain commentators have, however, doubted whether the Brussels effect does actually take place in the context of data protection. Lam interprets Bradford’s understanding of the Brussels effect as the CJEU “dictating” the content of the data protection legislation of the rest of the world (Lam 2017, p. 10). Furthermore, Schwartz goes on to claim that there is no unilateral regulatory globalisation EU data protection standards as the EU has always been open to negotiations concerning international

The next step for the Brussels effect is to not only affect the operators engaging in the processing activities on the European market, but to also affect the foreign legislators themselves to adopt data protection requirements similar to those of the GDPR, turning a *de facto* Brussels effect into a *de jure* Brussels effect.[309] For instance, such an effect was directly acknowledged when the Australian Privacy Act was amended in 2000. In the explanatory memorandum, it was noted that "There are serious questions surrounding the ability of Australia to meet the requirements for continued trade with EU Members under the [Data Protection Directive]".[310]

The obvious benefit of the Brussels effect is the fact that no coercion is involved in the globalisation of regulatory standards. On one hand, as the globalisation under the Brussels effect involves no coercion whatsoever and the foreign parties assume the EU rules voluntarily, no "forceful" assertion of jurisdiction is made, and therefore the effect cannot be contested as insufficiently justified. When a *de facto* Brussels effect occurs, the only sensible options for the states where such behaviour is observed are to either remain completely passive or to revise their own legislation to match the standards assumed by the operators[311] – as no forceful assertion of legislative jurisdiction is made, blocking action would seem overly defensive.

On the other hand, the list of prerequisites for the Brussels effect is long, and the effect cannot occur in any field of law.[312] Additionally, the lack of coercion involved in the Brussels effect can, at the same time, be considered as its disadvantage: as the main active role in the fulfilment of the Brussels effect is on the companies subject to regulation, the EU has no way of making sure that the Brussels effect does take place and result in

---

data transfers, failing to notice, however, that the negotiated solutions can also have a Brussels effect of their own (Schwartz 2013, p. 1987, 1990). Both of these commentators appear to disregard the wider perspective of the EU affecting the behaviour and legislation abroad, including the *de facto* Brussels effect, and fail to examine the relevance of the effect outside of the EU–US perspective.

[309] If the standards assumed by the foreign legislator are sufficiently close to the ones of the GDPR, adequacy talks can potentially be begun following a *de jure* Brussels effect. As noted above, an adequacy decision can greatly facilitate the data flows between the EU and the third state.

[310] C2004B00628, p. 13.

[311] Perhaps, due to the lobbying of the companies themselves aspiring to achieve a level playing field with their competitors not engaging in business activities on the European market (Bradford 2012, p. 6).

[312] See Bradford 2012, p. 10–11.

non-EU states adopting similar standards.[313] Despite these possible issues, the globalisation of EU data protection standards can be considered successful from the point of view of the EU: the Brussels effect, along with the abovementioned effect of bilateral negotiations and multilateral agreements have resulted in seeing the influence of European data protection regime in over 30[314] different national non-EU data protection laws.[315]

### 3.4 Other effects

Lastly, the EU data protection regime can cause even more subtle effects by influencing consumer behaviour, attitudes and awareness by the means of available information. As a result of the Snowden revelations, the Facebook–Cambridge Analytica data scandal, and the numerous news concerning large companies being involved in massive data breaches, more and more people are beginning to pay more attention to privacy matters.[316] These events, along with the additional privacy awareness caused by the enactment of the GDPR and the implementation of its requirements by the operators, are bound to "nudge" consumers towards "better" decisions, at least from a privacy standpoint: such nudging may result in, e.g., consumers becoming aware of and tinkering with their social media privacy settings or preferring more privacy-oriented online service providers. Such influence on the expectations and the behaviour of at least some consumers may, in the end, result in market pressure and a growing number of operators adopting better privacy standards,[317] paving the way for the growing, albeit less direct effect of the GDPR.

---

[313] It should also be noted that, as demonstrated by Petkova, globalisation of norms often goes both ways, with EU accepting certain US approaches relating to data breach notifications and data protection officers (Petkova 2018, p. 1150–1152, 1156).

[314] As of 2012.

[315] Greenleaf 2012, p. 74–75.

[316] According to certain surveys, majority of US consumers would like to have similar data protection safeguards as the one provided by the GDPR to consumers in the EU (SAS 2018, p. 4, see also nCipher 2019). It has been argued, additionally, that the plethora of information concerning data protection also affects the business practices of operators and is linked with the potential reputational damage of non-compliance (for further reasoning, see Greze 21019, p. 112).

[317] Referred to as "double nudging". When a growing amount of companies adopt such standards, even the most passive consumers can be forced to adopt these standards – such a situation is referred to as "triple nudging" (see Halpern 2015, Chapter 7. Data and transparency – *Nudging me, nudging you* and *Obesity*).

It is clear that transparency and the dissemination of information can have a drastic effect on the behaviour and the decisions of data subjects[318] – hence "[processing] in a transparent manner" and "accountability" being some of the key principles in Article 5 GDPR. However, while it is important to acknowledge the existence of such an effect, it is less legislative and more sociological, as it is caused by the influence on human behaviour through information. Falling outside of the scope of this work, it will not be discussed here in further detail.

# 4 Assessment of the extraterritoriality of the GDPR

## 4.1 Is the EU data protection regime extraterritorial?

As discussed above, there are numerous different definitions to the concept of "extra-territoriality". Assuming different understandings of extraterritoriality, one could come to varying conclusions regarding the question in the heading of this section. For instance, when analysing the CJEU decision in *Google Spain*, some might claim that when an operator is found to have an "establishment" within the EU, there is nothing "extraterri-torial" about applying EU law to the activity of such an operator.[319] However, it cannot be overlooked that while Google did have an establishment in the EU, what the *Google Spain* judgment also concerned was the CJEU ruling in favour of applying EU law to Google Inc. located in Mountain View, California.[320] Therefore, stating that the judgment was purely territorial would be misleading – after all, the processing activity subject to regulation took place on non-European soil and was carried out by a non-European entity.[321]

Regardless of the notable cross-border effects of the EU data protection law, the term "extraterritorial" is rarely used by the EU officials and courts to describe its territorial scope.[322] CJEU has, however, acknowledged that due to the nature of protection

[318] Halpern 2015, Chapter 7. Data and transparency – *Conclusion: data transparency plus behav-ioural science can reshape markets, and often do a better job of it than conventional regulation.*

[319] Gidari 2014.

[320] While Google does have a substantial establishment in the EU, the broad interpretation of the "establishment" criterion implies that a much weaker connection between the operator and the Union could constitute an establishment, and, therefore, subject the non-European operator to the GDPR.

[321] Van Alsenoy & Koekkoek 2015, p. 110–111. According to de Hert & Czerniawski 2016, p. 234, the judgment in *Google Spain* in any event ascertained that the scope of the "establishment" criterion is not purely territorial.

[322] For instance, "extraterritoriality" is not mentioned in the recent EDPB Guidelines 3/2018 discuss-ing specifically the territorial scope of the GDPR.

granted by the EU data protection law and the risks associated with its circumvention, its territorial scope is rather broad.[323] While "extraterritoriality" of the EU data protection law as such is rarely officially acknowledged, the problems associated with overly broad territorial claims have already been recognised in the 2003 CJEU judgment in *Lindqvist*, which concerned the legal status of disclosure of personal data on a website and the definition of a transfer of personal data to a third country.[324] When assessing whether the availability of personal data to persons browsing the internet from outside the EU constituted a transfer of personal data to a third country within the meaning of Article 25 of the Directive, the Court found, essentially, that it was not intended for the directive to be applicable to all activity on the internet, and, therefore, that the mere availability of the personal data in a third country did not constitute a transfer that would fall within the scope of the Directive.[325] This finding constitutes that while the territorial scope of the Directive was broad, it was not reasonable to keep overly expanding it – continuous expansion might lead to a situation where, for instance, the EU essentially attempts to globally regulate all online conduct. Such a situation would be questionable and disproportionate, to say the least.

Despite the clear effects outside the EU, not all seem to agree whether the EU data protection regime is indeed extraterritorial, or, at least, to which extent it is extraterritorial. At times, European commentators belittle the GDPR's extraterritoriality,[326] whereas the non-Europeans often view the EU data protection rules as strongly and even overly extraterritorial.[327] Such behaviour reflects a logical and expected situation: the party making an extraterritorial claim attempts to downplay the extent of its assertions in order to facilitate its justification, whereas opposing parties may, on the contrary, attempt to aggrandise the assertions in a defensive attempt to thwart them.

In this work, I have assumed the broad definition of extraterritoriality mentioned above – extraterritoriality, on one hand, as a state's endeavour to control the activities of a

---

[323] Opinion of Advocate General Jääskinen in C-131/12 – *Google Spain and Google*, delivered on 25 June 2013, para 28–29; C-131/12 – *Google Spain and Google* para 54; C-230/14 – *Weltimmo*, para 27; see also Svantesson 2016b, p. 335.

[324] C-101/01 – *Lindqvist.*

[325] C-101/01 – *Lindqvist*, para 69–70.

[326] See, e.g., Poullet 2007, p. 148–149, claiming (in relation to the Data Protection Directive) that only Subparagraph 4(1)(c) bears an extraterritorial scope. Poullet argues, for instance, that the Directive's provision concerning international data transfers do not have an extraterritorial impact, as the situations targeted by these provisions are "only ones clearly located in Europe".

[327] See, e.g., US Congress 2001, where numerous commentators highlight the extraterritoriality of the EU data protection requirements.

natural or legal person situated outside its borders,[328] and, on the other hand, as the factual effects on the activity of persons outside a state's borders regardless of the state's intent.[329] Such a definition is suitable for the purposes of this assessment as the aim of this work is to form an overall picture of the EU's ways to influence the data processing activity outside its borders. Using this definition, it is possible to conclude that actually, the GDPR appears to employ multiple different ways in which it has a *de facto* extraterritorial effect, with some of these ways being more direct than the others – in fact, all of the mechanisms discussed above in section 3 have a certain kind of effect on the behaviour of non-EU entities.[330] Due to some effect abroad being achieved under all of these approaches, it should be discussed which ones of these effects serve the purposes of the EU data protection law best, and which of them are sufficiently justified relative to their results.

The extraterritorial assertions made in the GDPR are characterised by the EU's intention to create a level playing field between the domestic and foreign parties engaging in data processing operations on the EU market,[331] and the aim to ensure an adequate level of protection for all natural persons within the EU.[332] Additionally, the broad assertions are often explained by the core nature of privacy as a right – as just a single incident involving unlawful access to certain information can cause irreparable damage, lax requirements abroad can cause a high risk to the security of personal data that is so diligently protected within the EU.[333] Therefore, it is clear that the EU's intentions are

[328] Svantesson 2015a, p. 227; Kuner 2015a, p. 238.

[329] See section 2.3 above.

[330] Hijmans has even concluded that "any intervention by the European Union with the purpose of ensuring privacy and data protection on the internet has extraterritorial effect" (Hijmans 2016, p. 504).

[331] Gömann 2017, p. 567–568; this was also highlighted in European Commission Vice-President Reding's speech of 4 March 2014, where she stated the following: "On territorial scope I recall the broad support that was voiced for making sure that non-European companies, when offering services to European consumers, apply the same rules and adhere to the same levels of protection of personal data as European companies. This is about creating a level playing-field between European and non-European businesses. About fair competition in a globalised world" (Reding 2014). Cf. Svantesson 2015a, p. 230–231, questioning this intention by arguing that costs of compliance with the GDPR would be too heavy for the smaller businesses not located in the EU, as a result of which only large non-EU businesses could afford to compete in the EU market. See also Tene & Wolf 2013, p. 2, stating that the outcome of the extraterritorial scope of the GDPR, combined with the one-stop-shop concept introduced by the Regulation, discriminates against organisations that are established outside the EU.

[332] This intention has already been stated in the preparation of the Data Protection Directive, see COM(92) 422 final – SYN 287, p. 13. See also recitals 1–3 of the GDPR.

[333] See, e.g., Opinion of Advocate General Jääskinen in C-131/12 – *Google Spain and Google,* para 28–29. For these reasons, the GDPR is not the only data protection regime in the world making extraterritorial assertions – similar assertions, at least to some extent, can be found in Australian,

appropriate and even laudable; the question that will be discussed next is, however, whether the means used to achieve them are proportionate and acceptable.

## 4.2 Are the extraterritorial claims justified?

### 4.2.1 Justification under EU law

As noted by Svantesson, when assessing the legitimacy and justification of an extraterritorial claims, one must first assess whether they are in line with domestic law of the state making the assertion, after which one can review the assertion from the point of view of international law.[334] While the purpose of this work is the normative assessment of the extraterritoriality of the GDPR in light of public international law, we can briefly review the internal justification of the extraterritorial assertions made in the GDPR in the light of relevant EU law.

In this case, I am assessing the assertions made in the secondary EU law, in particular, the GDPR. As with all secondary law, it is based on the primary EU law – namely, the TEU, TFEU and the Charter of Fundamental Rights.[335] As it is stated in Recital 1 of the GDPR, the subject matter of the Regulation is based on Article 8[336] of the Charter and Article 16(1) TFEU.[337] However, neither of these provisions directly require or provide for the extraterritorial application of the Regulation.[338] Advocate General Szpunar has assessed the domestic legitimacy of the extraterritoriality of the Directive, and, in particular, its extraterritorial enforcement, in his opinion in Case C-507/17. Basing his argumentation on Article 52 TEU and Article 255 TFEU, he concludes that outside the territory of the EU defined by the articles, "EU law cannot, in principle, apply or, consequently, create rights and obligations."[339] However, following this overview, Szpunar then acknowledges that despite the basic principle, extraterritorial effects are allowed

Singaporean, US and Canadian data protection legislation (see Azzi 2018, p. 131–132; Svantesson 2013b, p. 113–122; Svantesson 2015a, p. 227; Kuner 2010a, p. 192).

[334] Svantesson 2013b, p. 86–87.

[335] Article 288 TFEU, Talus & Penttinen 2015, p. 6–7.

[336] According to Article 8(1) of the Charter, "Everyone has the right to the protection of personal data concerning him or her."

[337] According to Article 16(1) TFEU, "Everyone has the right to the protection of personal data concerning them."

[338] It can be argued, though, that these provisions bear an implicit extraterritorial scope – if their application would be strictly restricted to the territory of the EU, the protection granted by the them would not be effective.

[339] Opinion of Advocate General Szpunar in C-507/17 – *Google*, delivered on 10 January 2019, para 47.

in EU law in certain situations, referring to settled case law in competition and intellectual property law matters.[340] Despite the settled case law, Szpunar views that such extraterritoriality of EU law should be viewed as an exception from the main principle, acknowledging, however, that it is difficult to make analogous interpretations in the context of omnipresent cyberspace.[341] Therefore, while the assertions of legislative jurisdiction made in the GDPR appear to be domestically legitimate, Advocate General Szpunar advises against the extraterritorial enforcement of such assertions considering their possible implications.[342]

### 4.2.2 Justification under international law

Next, I will move on to the examination of the justification of the extraterritorial claims made in the GDPR in the light of international law.[343] Above, I have examined the three core factors proposed by Svantesson that can be used to assess the justification of an extraterritorial claim: these are (i) the connection between the state making a claim and the matter, (ii) the legitimate interest of the state to assert jurisdiction over the matter, and (iii) the severity and proportionality of the assertion, all circumstances and competing interests considered. Due to the to the complex nature of data protection matters, I will use this approach in the following review.[344]

#### 4.2.2.1 Level of connection

Firstly, it should therefore be assessed whether there is a sufficient connection between the EU making an extraterritorial claim and the actual matter it wishes to regulate.[345] In

---

[340] Opinion of Advocate General Szpunar in C-507/17 – *Google*, para 50–52. See, for instance, a clear application of the effects doctrine in C-413/14 P – *Intel v Commission*, para 43. As regards the extraterritorial effects of regulation with a domestic trigger, such as the regulation of international data transfers under Chapter V GDPR, such effects were explicitly assessed and found domestically acceptable in C-366/10 – *Air Transport Association of America and Others*, reviewed above in note 102.

[341] Opinion of Advocate General Szpunar in C-507/17 – *Google*, para 53.

[342] Opinion of Advocate General Szpunar in C-507/17 – *Google*, para 60–61, 63.

[343] For the relationship between fundamental rights in EU law and the principles of international law, see note 164 above, discussing, *inter alia*, CJEU cases C-402/05 P – *Kadi and Al Barakaat International Foundation v Council and Commission* and C-584/10 P – *Commission and Others v Kadi*, in which the autonomous nature of EU law was highlighted.

[344] Svantesson 2015a, p. 227. For further information on these principles, refer to section 2.4.1 above. The complex nature of data protection matters has been exemplified in *Google Spain*, where the application of the Directive to California-based Google Inc. was based on the combination of territoriality and effects doctrine, making it difficult to assess the justification of the claim based on these principles alone (Van Alsenoy & Koekkoek 2015, p. 109).

[345] See also Hijmans 2016, p. 478–482, discussing what constitutes a meaningful link between the EU and a matter.

the cases where the EU directly attempts to control the activity of non-EU operator, such as under Article 3(2), the nexus for such control is the location of data subjects concerned in the EU. In the case of Article 3(1) or the regulation of international data transfers, the nexus is location of the establishment of the operator or the data exporter[346] respectively.[347]

While I have adopted a novel approach to the justification of extraterritorial claims, the Harvard Draft principles reviewed earlier can still be useful when assessing the level of connection between the EU and the matter it attempts to regulate. In addition to the effects doctrine, it has been argued that the introduction of Article 3(2) GDPR marked a move from objective territoriality as the connection between the state and the matter[348] towards passive personality, constituting a shift from a "controversial ground" to an even "more controversial ground".[349] In light of this observation, it can be concluded that the nexus between the EU and the matters it attempts to regulate under Article 3(2) is somewhat tenuous.[350] On the other hand, the more territorial-based connection implied in Article 3(1) and Chapter V appears to be much more firm.[351]

#### 4.2.2.2 Interests of the regulator

Secondly, an evaluation of the interest of the regulator performing the assertion should be made – the question is, therefore, whether the EU has a legitimate interest in regulating a certain matter formally within the scope of its data protection law. It has been claimed in connection with the "use of equipment" principle under Article 4(1)(c) of the Directive that in certain situations the EU's actual interest to regulate such processing might be rather low – why should the EU regulate, for instance, the processing of Indonesian data subjects' personal data carried out by an Indonesian controller using server

[346] Compare this with the theory of "territorial extension" proposed by Scott, see Scott 2014b, p. 90.

[347] For reasons discussed later in connection with the assessment of the reasonableness of extraterritorial assertions, certain cross-border effects of the GDPR, such as the Brussels effect, are not reviewed in this particular context.

[348] Referring to the "use of equipment" principle under Article 4(1)(c) of the Directive.

[349] Svantesson 2013b, p. 142–143.

[350] Ryngaert has implied that in certain situations, when a connection between the state and the matter is weak, the state should resort to exercise of its extraterritorial jurisdiction on a principle of subsidiarity, in case the state that has better possibilities to exercise jurisdiction fails to do so and the exercise of jurisdiction can be considered important from a global perspective. Such approach, however, applies better to, e.g., international crimes or competition law violations, which may have a direct harmful effect on a global scale (Ryngaert 2015a, p. 66 et seq.).

[351] Overly expansive interpretation of the establishment criterion can, however, undermine this connection.

space that just happens to be physically located in Europe?[352] As the provision allowed for Member States to regulate matters in which they had no real legitimate interest, it was argued that the it could have resulted in regulatory overreaching when applied to online environment.[353]

While the introduction of the GDPR did away with the "use of equipment" criterion and the questionable assertions of jurisdiction based on it, the territorial scope of the EU data protection law was further expanded by the introduction of the targeting criterion. However, the broad territorial scope under renewed Article 3(2) requires the application of EU data protection standards whenever data subjects located in the EU are targeted. As one of the main aims of the Regulation is to ensure the effective protection of data subjects in the EU, in the case of Article 3(2),[354] the EU's interest to regulate the processing activities is much higher than when attempting to regulate processing activities of a non-EU operator processing the data of non-EU data subjects under Article 4(1)(c) DPD.

The legitimacy of the EU interests is supported by the fact that the interest of promoting privacy and, consequently, the protection of personal data has been recognised rather widely. In addition to its status as a fundamental right within the EU, the right to privacy has been affirmed, *inter alia*, in the ECHR and the ICCPR, promoting the understanding of privacy as a universal human right. Later, the importance of data protection as a part of privacy was highlighted when numerous states ratified the Council of Europe Convention 108. In light of recent revelations concerning privacy violations all around the world, the widening scope of data protection related assertions of jurisdiction is therefore understandable.[355] Considering this universal recognition of the value of privacy, Simitis has even argued that it has never been the intention of the EU to become a "privacy cop" and globally impose its own privacy standards – instead, the EU has just been acting in compliance with the requirements of the Charter of Fundamental Rights

[352] Tene & Wolf 2013, p. 3–4. The issue has also been acknowledged by the WP29, calling the universal application of EU law caused by the "use of equipment" criterion an "undesirable consequence" (WP 179, p. 31). Earlier, the WP29 suggested that Article 4(1)(c) of the directive should only be applied in those cases, "where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-frontier situation involved" (WP 56, p. 9). Cf. Article 8(1) of the Charter and Article 16(1) TFEU providing that "everyone [regardless of nationality] has the right to the protection of personal data concerning him or her".

[353] Bygrave 2000, p. 255.

[354] See, e.g., Article 1 and Recitals 1 and 2 of the Regulation.

[355] Kuner 2015a, p. 242–243.

of the European Union.[356] While such view can be questioned, it is clear that the EU's values and interests behind the extraterritorial assertions of the GDPR are significant.

Additionally, the EU's interest to regulate cases both under Article 3 and under Chapter V GDPR is very much understandable considering the nature of data protection as a right – as described above, if there are lacunae in the level of protection, even a single incident of unlawful disclosure of personal data caused by them can have far-reaching consequences for the natural persons in the EU. Without extraterritorial claims, the data protection law would be essentially useless: firstly, relocation to areas with weaker level of protection would be possible for domestic operators, and secondly, overseas operators would get a significant competitive advantage over the operators based in the EU.[357] Extraterritoriality of the GDPR, on the other hand, provides, at least in theory, for a level playing field between both European and foreign operators.[358] For these reasons, it is possible to conclude that the interest of the EU to regulate matters falling within the scope of the GDPR is, indeed, substantial and legitimate.

#### 4.2.2.3 Proportionality of an assertion

Lastly, it should be assessed whether the EU's assertion of jurisdiction is reasonable and proportionate, considering all relevant circumstances and the proportionality of interests of the EU in relation to the interests of other legislators and parties – a balancing act, of some sort.[359] When assessing the reasonableness of an assertion of jurisdiction, one should first consider its severity. In this case, the matters to consider are, *inter alia*, how direct an assertion is, how much it encroaches on the exclusive prerogatives of other states, what are the differing interests of these other states, and what weight should be given to them.

In the case of direct assertions of jurisdiction over the conduct of operators situated abroad, such as under Article 3(2) GDPR, the EU must demonstrate that its interests

---

[356] Simitis 2010, p. 1992–1993. Such justification by the means of primary EU law relates, however, to the domestic law justification of the assertion, discussed in the beginning of this section. Therefore, justification of an assertion under international law cannot be made by a reference to a higher-level domestic regulatory instrument. See also Lynskey 2015, p. 43, arguing that that the increasing extraterritorial reach of the EU data protection regime is an organic development taking place as a secondary result of the EU international data transfer rules.

[357] Van Alsenoy & Koekkoek 2015, p. 110.

[358] Reding 2014. It is, however, not exactly clear whether the aim of creating a "level playing field" is really achieved, as the costs of compliance with the GDPR are high, causing some smaller foreign operators to withdraw from the European market, see Svantesson 2015a, p. 230.

[359] Svantesson 2015–2016, p. 71.

are strong and that they transcend the regulatory interests of third states, whose exclusive rights are being encroached on. On the other hand, if an extraterritorial effect is a merely incidental result of domestic regulation, the required level of EU's interest can be considered to be rather low. It can even be argued that in cases involving no extraterritorial coercion, no justification is required whatsoever. For this reason, it can be seen that the Brussels effect and the cooperatively prepared adequacy decisions need no justification at all in this respect.[360] The status of the regulation of international data transfers in this relation is somewhat unclear and appears to fall somewhere in between these two extremes – while it does have a direct effect on data importers outside the EU, it is aimed at the data exporters located within the EU.

As argued above, the universally recognised status of privacy as a right signifies the importance of the EU's efforts to protect data subjects within the Union and supports the finding that in this respect, the EU's assertions of jurisdiction are reasonable. Certainty, predictability and fairness can also be considered to form a part of reasonableness of an extraterritorial claim: for instance, the CJEU's approach involving subjective targeting[361] in relation to Article 3(2) GDPR has faced some critique, as basing the applicability of a law on a subjective intent can introduce some uncertainty to its application – it is not always unequivocal whether an operator actively endeavours to direct its activities to a Member State, and, even if the operator does, its endeavours may not result in the actual acquisition of any clients in the EU. For these reasons, it has been proposed that subjective viewpoints should not be considered when determining whether targeting takes place – instead, the assessment should be based on the actual outcome of the operator's activity.[362] On the other hand, it has been argued that the subjective targeting approach is also acceptable as due to its reasonable and fair approach to all operators endeavouring to do business in the EU.[363] While it is impossible to draw a

[360] For this reason, these effects were not discussed earlier in this section. Nevertheless, the adequacy framework has received its deal of criticism, see, e.g., Lam 2017, p. 10.

[361] See C-144/09 – *Pammer and Hotel Alpenhof*, C-190/11 – *Mühlleitner* and C-218/12 – *Emrek* discussed above in section 3.1.2.

[362] Svantesson 2015a, p. 232. Due to its focus on subjectivity, Svantesson even goes as far as arguing that in practice, the targeting approach is "useless" and undermines the legitimacy of the GDPR.

[363] Greze 2019, p. 110. A focus on the subjective intention of the operator can be considered appropriate for many reasons: on a general level, in the context of data protection, it does provide a better protection for the data subjects in the EU. On one hand, for the operators, it is easier to ensure compliance with EU data protection law before commencing business activities on the EU market – otherwise the operator should adjust its practices right after launch the moment the first data subject appears. On the other hand, ensuring compliance when endeavouring to process the personal data of individuals in the EU can be seen as a cost of entering the EU market. Such a cost can be considered to be a part of the general risk associated with any kind of business – client acquisition might

clear line and claim that one approach is more reasonable than the other, the extensive list of factors constituting targeting provided by the CJEU does ensure that the applicability of the targeting criterion is predictable and fair.

While the EU claims may seem completely reasonable from the European point of view, the competing interests of other legislators cannot be forgotten. For instance, as argued above, while the US does not have such a developed data protection framework as the EU does, freedom of speech is one of the US' core values, as secured in the First Amendment to the US Constitution. With freedom of speech being such a deep-rooted value, enforcement of, e.g., the right to be forgotten under EU law could turn out to be impossible under the heavy safeguards put in place in order to protect the freedom of speech.[364] For this reason, while the EU's data protection ambitions are based on internationally recognised human rights, the US valuing the right free speech over privacy can cause a real difficulty in the context of cases involving the right to be forgotten. As the right to free speech is also an equally recognised human right, the interest of the US may surpass the one of the EU on the US territory.

On the other hand, the interests of developing countries and weaker parties situated therein should also be considered – from their perspective, EU's approach to regulating data protection may even seem as an imperialist show of power.[365] While the area of extraterritorial assertions is filled with different extreme opinions and exaggerations concerning what is acceptable and what is not,[366] considering the principles of comity and sovereign equality, the competing interests and values of all other parties should be assessed and properly accounted for.

To finish this section, it should be reminded that it is a very serious claim to allege that an assertion of jurisdiction is exorbitant or that it is not in compliance with international law.[367] For this reason, it is possible to come to a generalising conclusion that an assertion of jurisdiction is, most probably, acceptable as long as nobody is "hurt" – if the EU

---

fail and, in the end, there might be nobody whose personal data to process (cf. Johnson et al. 2017, p. 34, 45–46).

[364] See the US SPEECH Act, Section 2, which, according to Wimmer, if interpreted broadly, provides that "all foreign judgments that would violate the First Amendment or chill free speech should be unenforceable through the U.S. court system if those cases are deliberately brought in jurisdictions whose laws are less protective of free speech" (Wimmer 2018, p. 574–575).

[365] Zielonka 2008, p. 475. This view has been disputed in Poullet 2007, p. 147.

[366] See, e.g., Lam claiming that "any exercise of extraterritorial jurisdiction undermines the international order" in Lam 2017, p. 10.

[367] Kuner 2010b, p. 241.

asserts jurisdiction over a matter and no other states oppose the assertion, the assertion is most likely acceptable and its justification should not be worried about.[368] It should also be reminded that in light of all of the many-sided circumstances reviewed above, it is probably not even possible to claim whether an assertion of jurisdiction is fully acceptable or entirely violating international law.[369] For this reason, it can be seen as a problem that the GDPR's requirements appear to apply extraterritorially in a black or white fashion[370] – this problem will be addressed later in section 4.4.1.

However, while it might not be possible to rule an assertion completely illegitimate, it should be kept in mind that any aspirations to globally regulate online activity, even if attempted for a good cause, cannot be accepted. Non-interference with unlimited extraterritorial assertions by a democratic nation could signal to other states that global enforcement of their own values would also be acceptable – in such case, quoting Advocate General Szpunar, "[t]here would be a genuine risk of a race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale."[371] As one of the limiting factors for such assertions, which can also be seen as a part of an assertion's reasonableness and as a safeguard of the Regulation's effectivity, it is possible to examine the enforceability of the extraterritorial claims made in the GDPR.[372]

## 4.3 Extraterritorial enforceability and enforcement of the EU data protection standards

### 4.3.1 Enforceability in the case of non-compliance of a non-European operator

As noted above, while the extraterritorial use of prescriptive jurisdiction may be accepted in certain contexts, the acceptability of the extraterritorial use of enforcement jurisdiction does not follow automatically – the basic principle regarding the use of enforcement jurisdiction remains that a state[373] cannot perform any enforcement

[368] Svantesson, for instance, proposes that the state asserting jurisdiction should also first consider whether it should refrain from an assertion by evaluating the whole picture: what would be the outcome of the assertion, how would other states react to it, and what positive or negative results may follow (Svantesson 2013b, p. 86–87).

[369] Such approach, according to Svantesson, is neither productive – alternative approach to this problem will be discussed in section 4.4 (Svantesson 2013a, p. 280).

[370] Kuner 2015a, p. 242.

[371] Opinion of Advocate General Szpunar in C-507/17 – *Google*, delivered on 10 January 2019, para 61.

[372] Azzi 2018, p. 127.

[373] Or, in the context of this work, the EU.

measures on the territory of another state.[374] The rule implies that no enforcement action on the part of EU can be brought outside of the territory of the European Union.[375] While it has been argued that it is not exactly apparent how much enforceability of a law really affects the extent to which a law is complied with,[376] it is clear that the overall efficiency of the EU data protection regime greatly relies on how well its requirements are honoured outside the EU.[377]

From the point of view of enforcement, the biggest challenge of the GDPR is its territorial scope under Article 3(2),[378] which is a problem already acknowledged by the WP29 in the context of Article 4(1)(c) of the Directive.[379] A number of issues have been identified in connection with the enforcement difficulties of the GDPR when it is applicable under Article 3(2):[380] for instance, if an EU court attempts to enforce a decision of a Member State DPA, the premise is that the implementation of the order can only be made by the domestic competent authority in the state where the operator is based – such authority is highly unlikely to apply the GDPR. Enforcement through a foreign court is neither a viable option: the foreign court is unlikely to apply the provisions of the GDPR due to, among other things, the conflict of laws issues and the rule of non-enforceability of foreign public law that is well-established in numerous jurisdictions.[381]

When considering enforcement of the DPA decisions, the legal status of representatives appointed under Article 27 is also somewhat unclear – the binding text of the GDPR does not directly set a liability for the EU representatives of foreign operators, whereas,

---

[374] Akehurst 1972–1973, p. 146; Currie 2008, p. 335–336; Kuner 2010b, p. 232.

[375] Greze 2019, p. 115.

[376] Bygrave 2014, p. 189.

[377] Greze 2019, p. 110. See also Hijmans 2016, p. 178, arguing that under Article 16 TFEU, enforcement by the DPAs constitutes an essential part of the EU data protection regime.

[378] Greze 2019, p. 110.

[379] WP 56, p. 15. While the ”use of equipment” criterion still maintained an objective territorial connection between the Member State and the operator abroad, namely the equipment in the Member State, when using the targeting criterion of the GDPR there is, potentially, no territorial connection whatsoever between the EU and the operator.

[380] In certain cases, these issues can also relate to situations where the GDPR is applicable under Article 3(1).

[381] Greze 2019, p. 115. See, for example, Supreme Court of Canada case *Google v Equustek*, where the Supreme Court ordered Google to globally deindex results in which a company was breaching the intellectual property rights of Equustek Solutions Inc (SCC: *Google Inc., v. Equustek Solutions Inc.*). The Canadian decision was then struck down and its enforcement was prevented by a Californian court (N. D. Cal.: *Google LLC v Equustek Solutions Inc*.). See Svantesson 2018, p. 124.

according to the recital 80, the representatives "should be subject to enforcement proceedings in the event of non-compliance by the controller or processor."[382] In addition, the EDPB has stated that the obligation to appoint a representative was put in place in order to fill the enforcement gap caused by Article 3(2): "To this end, it was the intention to enable enforcers to initiate enforcement action against a representative in the same way as against controllers or processors. This includes the possibility to impose administrative fines and penalties, and to hold representatives liable."[383] This approach has faced critique, as the wording of the actual provisions of the GDPR suggests that the representatives could not be held liable for the non-compliance of the operators that designated the representative – as opposed to certain situations where the representatives are explicitly mentioned as having a certain obligation, they are not mentioned in the context of liability for non-compliance.[384] It can therefore be considered highly questionable to impose a potentially multi-million euro liability on a representative without a clear provision explicitly allowing for it and based only on non-binding normative material.

Additionally, when considering enforcement action aimed at a representative of a non-EU operator, the nature of the enforcement action must be accounted for. If an operator ordered to pay a mere monetary sanction, enforcement can (in practice) be sought against the representative. Whereas, when the enforcement concerns a performance of a specific obligation, such as the compliance with a request concerning the use of a data subject right, there is little a representative can do if all processing activities are managed outside the EU. In fact, a similar problem arises in connection with enforcement of judgments or DPA decisions concerning operators located outside the EU but having an establishment in the EU and that are thus subject to the Regulation under Article 3(1). As noted in *Weltimmo*, mere "stable arrangements" regardless of their legal form can constitute an establishment in a Member State.[385] If a non-EU operator is

[382] Recitals in secondary EU law cannot, however, be granted the status of an independent source of law (Köndgen 2017, p. 141–142).

[383] EDPB Guidelines 3/2018, p. 23. EDPB also noted that while the representative could be held liable, such liability does not affect the liability of the operator itself.

[384] Greze 2019, p. 124. Greze additionally points out the possibility of variance in the representatives' liability in accordance with Member State laws, with, for instance, Belgium law foreseeing civil liability and the matter remaining unclear in many other jurisdictions.

[385] C-230/14 – *Weltimmo,* para 28–31.

deemed to have an establishment similar to the one in *Weltimmo*, no enforcement action can be brought against it due to the lack of the operator's actual legal presence in the EU, in which case neither monetary nor performance obligations can be enforced.[386]

It can therefore be concluded that the enforceability of the GDPR, when it applies to fully non-European operators under Articles 3(2) and, in some cases, under Article 3(1), is rather uncertain. The unenforceable assertions have faced vigorous criticism: for instance, according to Kuner, the official recognition of enforcement difficulties by WP29 make the assertions exorbitant.[387] Additionally, while Svantesson acknowledges that, firstly, unenforceable laws can have certain symbolic and deterrent effects,[388] secondly, that whether an assertion is overreaching depends on its moral justification, and thirdly, that unenforceability is not a big issue if it concerns less important parts of a law, he concludes that these exceptions are not relevant in the context of the Regulation (and the Directive). Considering the broadness of the assertions made in the GDPR and the burdensome nature of some of the requirements of the GDPR, he concludes that it cannot be considered a legitimate use of "bark jurisdiction". Instead, he views that the overly broad claims of jurisdiction can, at worst, cast a negative light on the EU data protection regime and, eventually, undermine its legitimacy.[389]

### 4.3.2 Relationship between the territorial scope and regulation of international data transfers

Another significant issue that needs addressing in connection with the enforceability of the GDPR is the relationship between the Regulation's territorial scope under Article 3 and the regulation of international data transfers under Chapter V – as it has been noted before, the applicability of the Regulation under Article 3 and under Chapter V can sometimes overlap. For this reason, the approach has been dubbed a "belt and suspenders" approach – it might be more secure from a European point of view, but, as

[386] Greze 2019, p. 125. On the contrary, where a non-EU operator has an establishment in the EU in the form of a subsidiary or other legal person, financial penalties can be levied against these establishments even though the operator subject to fine is situated outside the EU, see, for instance, CNIL deliberation SAN-2019-001, p. 28, issuing a penalty of EUR 50 million against California-based Google LLC., but notifying the decision for its execution to the EU-based Google France SARL.

[387] Kuner 2010b, p. 236.

[388] Referring to his often-quoted concepts of "bark jurisdiction" and "bite jurisdiction".

[389] Svantesson 2015a, p. 233; cf. Hijmans 2016, p. 505.

these requirements do not appear to be coordinated with each other, the approach has been criticised as making little sense as a legislative framework.[390]

Despite the system adopted in the GDPR not being ideal with the possibility of regulatory overlaps, it cannot be denied that the data transfer mechanisms under Chapter V serve a more specific and nuanced function when compared to Article 3. Where the territorial scope under Article 3 establishes the general applicability of all of the requirements of the GDPR, the data transfer mechanisms provide some more specific and practical requirements and safeguards that the data importers outside the EU should comply with.[391]

As discussed above, at the core of each of these "appropriate safeguards" is their enforceability, which makes clear why the regulation of international data transfers has been kept separate from the general territorial scope of the Regulation, despite the possible overlaps between the two. On one hand, personal data that has been initially collected by a European operator, fully and indisputably subject to the GDPR, cannot escape the influence of the GDPR by being transferred abroad. If one were to consider the processing of EU individuals' personal data that has been collected outside the EU, the GDPR would apply to such processing in its entirety pursuant to Article 3. However, while all of the GDPR provisions would be applied, such an approach might not be ideal from the EU's perspective as the enforceability of the requirements would not be certain,[392] and, therefore, the level of protection provided by them might not necessarily be sufficient. On the other hand, while the subject matter requirements of the safeguards used when transferring the personal data outside the EU are not identical to those of the GDPR as whole and can contain certain trade-offs, these instruments are enforceable, guaranteeing the efficiency of the requirements contained therein.[393]

[390] Kuner 2015a, p. 244. Kuner even argues that the current dual regime of the GDPR should be replaced with a single coordinated one with no overlaps.

[391] For instance, the use of Standard Contractual Clauses adopted by the European Commission requires the data importer and exporter to enter into an agreement concerning the transfer, which, as opposed to the broad and contested assertion of jurisdiction under Article 3, can at a later point be fully enforced in case of non-compliance.

[392] Svantesson 2013a, p. 285.

[393] Schwartz 2013, p. 1987. For a famous example of trade-offs, see, for instance, the derogations provided for US-based operators under the Safe Harbour framework discussed above.

### 4.3.3 Extraterritorial implementation of data protection requirements

The last issue to be reviewed in this section, in addition to the enforceability of the EU data protection requirements, is the territorial scope of the implementation of the requirements of the GDPR. Therefore, as opposed to the *enforceability* examined above, I will discuss the *actual enforcement* of the Regulation next. As it will be described below, the issue of the territorial extent of enforcement of EU data protection standards is most relevant in the context of the implementation of the data subject rights, which is why the question will be assessed here in the context of the right to be forgotten.

While *Google Spain* was a landmark case concerning the right to be forgotten and the territorial scope of the EU data protection law, it did not provide guidelines as to what is the territorial extent of the fulfilment of a data subject's right to be forgotten.[394] As a result of the decision, Google removed the relevant results only from the European search pages in a way that the results could all still be accessed from the EU by using the international .com version of the results page.[395] However, the issue was later addressed by WP29, which found that in order to effectively protect the rights and freedoms of data subjects, "limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment [in *Google Spain*]."[396] If the delisting is carried out only on the European versions of the results pages, anyone could still access the information by using the international site, which undermines the whole idea of the right to be delisted.

As a result of the pressure authorities put on Google, the territorial extent of the right to be delisted was extended: in 2016, Google announced that, in addition to its previous delisting practices, it introduced geolocation signals to locate the users viewing the search results page, and that a delisted search result would not appear in the results viewed by users located in the same EU Member State as from which the request to be delisted came from, regardless of the domain version used.[397] From the European point of view, such an approach was a step in the right direction, but it still failed to provide full protection of data subject interests: geolocation could still be circumvented by the

[394] Kuner 2015b, p. 29, later acknowledged in the Opinion of Advocate General Szpunar in C-507/17 – *Google*, delivered on 10 January 2019, para 45.

[395] Van Alsenoy & Koekkoek 2015, p. 105–106.

[396] WP 225, p. 8–9.

[397] Google 2016.

use of a Virtual Private Network, and the results were still easily viewable by anyone that is not located in the same EU Member State as from which the request originated.[398]

For these reasons, such implementation was not enough for CNIL – it required Google to implement the right to be forgotten globally. Google did not comply with this requirement and contested the penalty it was issued for non-compliance in the French Conseil d'État, which referred the case to the CJEU. Essentially, Conseil d'État asked the Court whether a search engine operator is obliged to perform de-referencing on a global scale so that the information concerned would not appear even for those users who are outside the EU.[399]

In its decision, the Court affirmed[400] the existence of the data subjects' right to be delisted as regards internet search results[401] and that upheld the earlier findings concerning the applicability of the EU data protection law to Google's processing activities.[402] While the Court conceded that global de-referencing would provide the data subjects in the EU with the highest level of protection in accordance with the objectives of the DPD and the GDPR,[403] the Court acknowledged that in other jurisdictions the approach and the values related to the right to be forgotten can be different, calling for balancing of the right to the protection of personal data against other fundamental rights.[404] When balancing the rights, the Court pointed out that neither the provisions of the DPD nor the GDPR imply that the de-referencing should be carried out on a global scale.[405]

---

[398] Taylor 2017, p. 202, 204.

[399] C-507/17 – *Google*, para 30–39.

[400] The case was examined in the light of both the DPD and the GDPR (C-507/17 – *Google*, para 41) and taking into account the relevant case law, particularly *Google Spain* discussed above.

[401] C-507/17 – *Google*, para 44–47.

[402] C-507/17 – *Google*, para 48–51.

[403] C-507/17 – *Google*, para 54–57; see also Opinion of Advocate General Szpunar in C-507/17 – *Google*, delivered on 10 January 2019, para 36.

[404] C-507/17 – *Google*, para 59–60; Opinion of Advocate General Szpunar in C-507/17 – *Google*, delivered on 10 January 2019, para 57 (see para 54-56 for fundamental rights related reasoning); see also Opinion of Advocate General Jääskinen in C-131/12 – *Google Spain and Google*, delivered on 25 June 2013, para 120–125. Despite Advocate General Jääskinen's suggestions, the original *Google Spain* judgment was criticised for its lack of such balancing (Kuner 2015b, p. 41–42).

[405] C-507/17 – *Google*, para 62. In para 63, the Court also found that while there are mechanisms in the GDPR that allow for cooperation between Member State DPAs in order to establish the correct scope for de-referencing, there are no such mechanisms as regards establishing such scope outside the EU.

Hence, the Court found that the "operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States".[406] While the CJEU, as opposed to the Advocate General Szpunar,[407] did not explicitly refer to the use of geo-blocking techniques when complying with a de-referencing request, the Court instead stated that an operator should use, to the extent necessary, measures that "effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States" – the use of geo-blocking can be considered to belong to this group of measures.[408] While it is clear that such an approach does not guarantee the maximum level of protection to data subjects in the EU, it does make sense from the viewpoints of comity and balancing of fundamental rights: a decision requiring global de-referencing would substantially encroach on the prerogatives of other states.

While Advocate General Szpunar advised strongly against global implementation of the right to be forgotten,[409] the Court took a more moderate stance stating that while such global de-referencing is not required under EU law, it is neither prohibited. According to the judgment, "a supervisory or judicial authority of a Member State remains competent to [order] the operator of that search engine to carry out a de-referencing concerning all versions of that search engine", if the authority finds it appropriate after balancing the right to freedom of information and the data subject's right to privacy.[410] The Court's statement raises some questions concerning the actual impact of the judgment – if a Member State authority or a court can order global de-referencing of personal data and still be fully compliant with EU data protection law, what is the actual function of the judgment?[411] Such court order would, at worst, make it possible for the Member State authorities to try to interfere in the internet use of persons located outside the EU to

[406] C-507/17 – *Google*, para 73.

[407] Opinion of Advocate General Szpunar in C-507/17 – *Google*, para 78.

[408] C-507/17 – *Google*, para 73. As demonstrated in para 42, a geo-blocking mechanism was already implemented in the Google search engine at the time of the proceedings, making it much more difficult for users to switch between different localised versions of Google Search.

[409] Opinion of Advocate General Szpunar in C-507/17 – *Google*, delivered on 10 January 2019, para 46, 60–63. While in para 62, Advocate General Szpunar does consider the possibility that in certain cases, the application of the EU data protection law would be required due to the interest of the EU, it is clear that such derogation would not concern the global application of the right to be forgotten.

[410] C-507/17 – *Google*, para 72.

[411] In its reaction to the judgment, CNIL found that based on the para 72 of the judgment, "a supervisory authority, and so the CNIL, has the authority to force a search engine operator to delist results on all the versions of the search engine if it is justified in some cases to guarantee the rights of the individuals concerned" (CNIL 2019).

whom such an authority has no real connection and give rise to the risks of sending a questionable message to non-EU countries and race to bottom in the freedom of expression identified by Advocate General Szpunar.[412]

For this reason, it still remains unclear what are the true implications of the CJEU judgment in *Google.* On the surface, the judgment can be considered as a voice of reason from the Court: CJEU acknowledged that while the right to the protection of personal data is very highly valued in the EU, this might not be the case outside the EU.[413] However, when assessed on a deeper level, the possibility of derogation expressed at the end of the judgment appears to, at least to some extent, annul the court's other conclusions. Therefore, it remains to be seen how the territorial extent of data subject rights under the GDPR will develop in the future, and whether the Member State authorities will resort to the possibility of global enforcement granted to them in the judgment.

As it has been discussed above, the extraterritorial enforceability of the GDPR when it applies under Article 3(2), and, sometimes, Article 3(1), is uncertain, especially in cases with operators having no assets whatsoever within the EU. While the possibility of holding the designated representative of a non-EU operator accountable for the non-compliance of the operator has been raised, potentially levying a substantial liability on such representative without a clear legislative authorisation would not be in conformity with the principle of legal certainty. Additionally, while there have been some successful attempts at cooperation in the field of data protection, substantial results concerning the enforcement of the GDPR outside the EU are yet to be achieved.[414] As regards the actual enforcement of data subject rights, the direction taken by the Court can be considered sensible yet cautious: while the EU data subjects are not given a maximum level of protection, the judgment in C-507/17 – *Google* can be seen to consider[415] the global

[412] Taylor 2017, p. 205; Opinion of Advocate General Szpunar in C-507/17 – *Google*, para 61. As a blunt example, one could even argue that guided by success of global de-referencing orders in the EU, authorities in China could order Google do globally de-reference all search results related to the Tiananmen Square Massacre. While such an order, let alone the compliance with it, is rather unlikely, the possible effects of permissiveness towards global de-referencing should be borne in mind. See also Kohl 2007, p. 199.

[413] It should be noted, though, that while Advocate General Szpunar assessed the justification of the extraterritorial effects of the EU data protection law (see, e.g., para 47–57 of the Opinion of Advocate General Szpunar in C-507/17 – *Google*), the Court's reasoning relied only on the text of the relevant provisions of the DPD and the GDPR, and the balancing of fundamental rights.

[414] See Greze 2019, p. 116–117. Greze points out, for instance, the establishment of the Global Privacy Enforcement Network based on the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy and the successful cases of joint investigations concerning data processing practices of WhatsApp and Google. See also Hijmans 2016, p. 502–503.

[415] See, e.g., note 404 above.

influence of the EU data protection regime and the implications a global implementation the right to be forgotten could have.

However, considering the enforceability issues related to the GDPR, the level of protection granted by the EU data protection law may fall short of what was envisaged while drafting the GDPR. In the next section, I will examine the possible solutions to these issues faced by the Regulation.

## 4.4 A possible way forward?

The extraterritorial assertions made in the GDPR are not accepted by everyone. While it is not possible to say directly that some of these assertions are exorbitant and constitute "regulatory overreaching", it is possible to conclude that they are, due to their broad nature and uncertain enforceability, somewhat questionable – enforcement difficulties can undermine legal certainty and, in the end, even the legitimacy of the Regulation as viewed by non-European operators. It is clear that some work needs to be done when considering the future approach to the extraterritoriality of the EU data protection law: on one hand, the rights and freedoms of data subjects in the EU should be effectively protected, which is difficult without an extraterritorial reach of the data protection law, while, on the other hand, indiscriminate disregard of other sovereign regulators' powers, values and interests can neither be accepted. As argued by Kuner, the balancing of interests of all involved parties and the principle of comity should be considered in order for the legal certainty to be retained in the application of data protection legislation.[416] For these reasons, this section will focus on potential ways of approaching the problems with the Regulation's extraterritoriality reviewed above.

### 4.4.1 Gradual applicability of the data protection legislation

As identified earlier, the black or white applicability of the EU data protection law to non-European operators can be considered problematic.[417] Indeed, it can be viewed as unfair that if an online service operator aims at a global market, not only should its data protection practices fully comply with all detailed requirements of the GDPR, but also with all of the requirements of each of the other states, markets of which it is targeting. For this reason, it has been suggested that the applicability of data protection law, in this case, the GDPR, should be made more flexible by assuming a more nuanced, risk-

[416] Kuner 2015a, p. 245.
[417] Kuner 2015a, p. 242.

based, context-specific, and perhaps even gradual approach when assessing whether the Regulation should apply to a non-European operator.[418] Additionally, a proper introduction of jurisdictional "safety valves" described by Scott[419] could also make the extraterritorial applicability of the GDPR more flexible.

Following the "layered approach" proposed by Svantesson,[420] it could be argued that the data protection obligations of the GDPR could be divided in different categories,[421] with only certain elements forming the core of the right to protection of personal data.[422] According to Svantesson, these types of obligations could then be applied to non-European operators in a layered fashion so that those operators who have the biggest connection to the European market would be subject to most strict requirements, while the operators with less connection to the EU could just adhere to the core obligations.[423]

In his example, Svantesson divides the obligations of the EU data protection law in three layers: the "abuse-prevention layer", the "rights layer" and the "administrative layer". The core of the right to data protection, or the "abuse-prevention" layer of data protection, would consist of basic rules and principles preventing the unauthorised processing of personal data – these are the collection limitation, purpose specification and use lim-

[418] Kuner 2013, p. 183–184, calling for flexibility in the application of international data transfer regulation; according to Svantesson 2013a, p. 280, however, reasonableness in all of data protection law could be achieved by adjusting the criteria for extraterritorial application of each of the requirements separately based on their importance.

[419] Scott 2014a, p. 1345; these "safety valves" were discussed above in section 2.4.3.

[420] Svantesson's "layered approach" is, of course, only one of the numerous different approaches proposed in order to develop the extraterritoriality of the EU data protection law; see, e.g., Reed 2012, 229–232 and 241–242, suggesting generalisation of data protection law provisions for it to be better adaptable to different business models and for the compliance to be based on the operator's reasonable belief of compliance – according to Reed, while such approach does appear less certain than the existing laws, it is a trade-off that has to be made in order to effectively influence the behaviour of "cyberspace actors" often operating without legal advisers.

[421] Svantesson 2013a.

[422] Svantesson 2013a, p. 280–281; Kuner 2015a, p. 243–244.

[423] There is currently one example of a similar approach in the Regulation itself: according to Article 27(1), a non-European operator should designate a representative within the EU if the GDPR applies to the operator pursuant to Article 3(2). However, according to Paragraph 2, there is no obligation to designate a representative if the processing is, among other things, "occasional" and "unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing" – in other words, if certain conditions concerning the extent of targeting are not met, the burdensome requirement of designating a representative does not apply to a non-European operator (Svantesson 2018, p. 118–119). Additionally, some sort of scalability of obligations is visible even within the EU: for instance, under Article 37, only some operators need to appoint a data protection officer depending on the nature of their processing activities, and under Article 35, not all processing activities require a data protection impact assessment to be carried out in advance.

itation principles found in the OECD Privacy Guidelines (1980). Even a minimal connection with the EU would require compliance with these basic principles, and the enforcement of these principles could be carried out by the means of the EU's "market destroying measures" – e.g., by the means of restriction of market access and imposition of trading limitations.[424]

Next layers of data protection requirements in Svantesson's example are the "rights layer" and the "administrative layer", with the former including the data subjects' rights concerning e.g. operators' accountability and data accuracy, integrity and confidentiality, and with the latter concerning additional operators' obligations that can be classified as administrative, such as the obligation to appoint a data protection officer or the requirements concerning data protection by design and by default. These requirements would become applicable when an operator has a certain minimum level of contact with the EU – in the case of the "rights layer", when the operator "purposefully avail[s] itself of the privilege of conducting activities within [the EU], thus invoking the benefits and protections of its laws", and, in the case of the "administrative layer", when the operator's connection with the EU is "substantial, continuous and systematic to make the exercise of extraterritorial jurisdiction reasonable."[425]

While Svantesson's layered approach does provide for reasonableness and flexibility from the viewpoint of non-European operators, it jeopardises, at least to some extent, the level of protection granted to data subjects in the EU, as not all operators are obliged to achieve the same level of compliance with EU requirements. This becomes especially evident when the "abuse-prevention layer" is examined in contrast with Article 8 of the Charter – according to Svantesson, access and rectification rights codified Article 8(2) would belong to the "rights layer" requiring purposeful targeting on the part of the non-European operator, thus, making certain elements of Article 8 more important than the

[424] Svantesson 2013a, p. 281–282.

[425] Svantesson 2013a, p. 281, 283–284.

others.[426] It might be, therefore, appropriate to define the core of the right to data protection as it is defined in Article 8[427] – this would, however, make the core of the right to data protection rather broad and the utility of the "layered approach" questionable.

While such a layered approach would, most likely, make the EU data protection law more fair and proportionate from the viewpoint of non-European operators, there appear to be multiple issues related to the approach that would definitely need to be tackled first: How do data subjects stay aware what rights they have in relation to each of the operators they are dealing with? Can derogations from the Charter be made if the operator's connection to the EU is tenuous as a result of, e.g., global market being targeted? Is it fair and reasonable to apply different standards to different operators dealing with European data subjects? Although there already is some scalability to the obligations under the GDPR, the adoption of a layered approach would require a substantial amount of specification work[428] and would create a tremendously complex ecosystem that, along with its attempts to define different levels of connection and targeting in order to preserve predictability and legal certainty, would probably create more questions and uncertainty that what it could resolve.[429] Additionally, considering that the General Data Protection Regulation is a rather new regulatory framework as such, a complete legislative reform in order to assume a layered approach is highly unlikely anytime soon. Consequently, it seems necessary to work out a solution that is, on one hand, either fully compatible with the current law in force or requires only slight amendments, and, on the other hand, which accounts for the issues with extraterritoriality of the EU data protection regime reviewed above.

### 4.4.2 Emphasis on "friendly" extraterritoriality

It is clear that there a much fewer restrictions on extraterritorial assertions of legislative jurisdiction than enforcement jurisdiction, and, therefore, it is understandable that legislative assertions of the GDPR are somewhat broader than what can reasonably be expected to be enforced. While the significance of enforceability has been contested, it

[426] On the other hand, the purposeful targeting criterion can be viewed as equivalent to the one currently in use under Article 3(2) GDPR, whereas the territorial scope prescribed to the "abuse-prevention layer" under Svantesson's proposition would be even broader, as compliance with these top-level requirements would be compulsory at all times when EU data subjects' personal data is processed (Svantesson 2013a, p. 282).

[427] Hustinx 2013, p. 17–18.

[428] Svantesson 2013a, p. 280–281; Kuner 2015a, p. 244.

[429] See Reed 2012, p. 229.

cannot be denied that completely unenforceable legislative assertions may weaken the non-European public's and operators' perception of the European data protection law.[430] Therefore, it can be concluded that the legislative assertions made in the GDPR should be supported by the possibility of some kind of enforcement action.

When attempting to regulate the activities of operators outside the EU, special emphasis should be placed on the use of mechanisms that are either enforceable locally within the EU or that have an effect with no enforcement action concerning them.[431] The first group of extraterritorial mechanisms includes the use of the data transfer regulation under Chapter V of the regulation and the use of the establishment criterion in cases where an operator has some legal presence in a Member State.

While there are certain issues associated with the broad interpretation of the establishment criterion, basing jurisdiction on a slight territorial nexus can still be seen as more acceptable than when an assertion is made based on the targeting criterion. However, in terms of enforceability, the use of the enforceable safeguards for data transfers would probably be the most secure option from the European point of view. It should therefore be considered whether certain similar safeguards should be required from non-European operators performing the initial collection of personal data – an extreme solution might be to extend the representative requirement under Article 27 of the Regulation so that the collection of personal data would be carried out through the EU-based representative, and the subsequent transfer outside the EU should follow the principles set out in Chapter V. However, while such an approach could better guarantee the compliance with the Regulation outside the EU, it would form an even larger threshold for non-European operators to attempt to enter EU market, essentially depriving it of its viability.

It can be concluded that while the further expansion of the scope of the GDPR would provide the data subjects in the EU with a better and more effective level of protection, these requirements would not be fair for non-European operators. For these reasons, special attention should be paid another group of extraterritorial mechanisms. This

[430] As argued above in section 2.4.2, this could, at worst, further diminish the compliance with the unenforceable EU data protection standards.

[431] Hijmans argues that the effective enforcement of the EU data protection standards requires the selection of appropriate legislative instruments by the legislator and implies that effectivity of the enforcement should be evaluated based on whether EU retains control over the personal data (Hijmans 2016, p. 179). While Hijmans' arguments mainly concern the enforcement of the EU data protection law within the EU, these findings can also be extrapolated to also concern the enforcement of the GDPR abroad.

group consists of the mechanisms that involve close to no coercion on the part of the EU, and includes the mechanisms such as the bilateral adequacy cooperation, development of and adherence to multilateral treaties such as the Convention 108, and the unilateral regulatory globalisation. While the effect of these mechanisms can be less certain than the effect of the domestically enforceable ones, a non-aggressive message sent to other actors in the international field may encourage cooperation and be less likely to spark international conflict and blocking action.[432] Additionally, as pointed out before, transnational cooperation in the field of privacy enforcement is also possible, albeit yet not sufficiently developed – work on such cooperation could enhance the effects of the other extraterritorial mechanisms of the GDPR, as well.[433]

But then again, while the use of these friendly and non-intrusive regulatory techniques may be a good solution from the point of view of maintaining international order and diplomatic relations, it will certainly not provide the data subjects within the EU with a sufficient level of protection of their personal data in case of non-compliance. For this reason, as a last resort, while certain DPA decisions and orders might be unenforceable outside the Union, the EU could take action in order to restrict the market access of the operators deliberately breaking the requirements of the GDPR by, e.g., blocking their websites in the EU.[434] While this would be a rather severe type of action, Svantesson views such exercises of market sovereignty as an approach that is "much more sophisticated and targeted" when compared to attempts to regulate global activity,[435] and the effectiveness of such market access restrictions could be quite significant considering the importance of the EU market to many multinational data-oriented companies.[436]

[432] Such as the one described above in the dispute between Equustek and Google, see note 381.

[433] See also Hijmans 2016, p. 487, 490–493, supporting the reliance on Brussels effect and the globalisation under Convention 108 to unilaterally export the EU data protection standards. Hijmans acknowledges, however, the possibility of bilateral and multilateral cooperation in the field, and suggests that a UN treaty concerning data protection might, in the end, offer the best overall level of protection (Hijmans 2016, p. 508).

[434] See Greze 2019, p. 126. While not an enforcement measure specifically provided for in the Regulation, it is viewed to be a part of the EU's market sovereignty.

[435] Svantesson 2017, p. 147–148; as regards "market destroying measures", see also Svantesson 2013a, p. 282.

[436] However, when implementing such market blocking measures, the risk of fragmentation of the internet should be borne in mind (Davenport 2019; see also Kohl 2007, p. 199).

# 5 Concluding remarks

Over the course of this work, I have performed a critical examination of the various extraterritorial mechanisms in use as a part of the EU data protection law. The research questions of this work were aimed at, on one hand, the doctrinal examination of the extent of extraterritorial mechanisms of the GDPR, and, on the other hand, at the critical evaluation of said mechanisms in the light of public international law.

It is clear that due to the nature of the online world, strict adherence to the principle of territoriality can, at times, be very impractical or even devoid of meaning. As discussed above, in the context of data protection, basing standards on pure territoriality would significantly undermine the level of protection and the general aims of a data protection law – operators could just relocate to data havens and completely evade strict data protection requirements in their home country. These reasons have prompted legislators all around the world to enact data protection requirements reaching beyond the states' geographical borders, and, as it has become clear over the course of this work, the data protection regime of the EU is no exception.

As discussed in section 3, there are multiple different ways in which the influence of the GDPR reaches beyond the borders of the EU. While the Regulation has a very broad territorial scope that applies to a significant number of operators outside the EU – namely, those who have an establishment within the Union and those who target individuals in the Union – its effects outside EU borders do not end there. In addition, the GDPR has an effect on operators receiving personal data from a data exporter in the EU, even if such operators are otherwise not subject to the GDPR under its territorial scope. Furthermore, the European influence abroad is visible through the European Commission's adequacy decisions, bilaterally and multilaterally negotiated instruments, the Regulation's Brussels effect and even the public awareness concerning privacy matters that has been affected, at least indirectly, by the strict requirements of the EU data protection law.

In the light of the pragmatic definition of extraterritoriality assumed in section 2, I concluded that all of these effects can indeed be considered extraterritorial. After inspecting these effects from the viewpoint of public international law, I was able to conclude that

some of these effects can be considered more “reasonable” than others.[437] Especially, when one considers the proportionality and the enforceability of extraterritorial claims, certain mechanisms stand out: for instance, if an Asian business targets a global market and processes the personal data of data subjects in the EU, such operator is likely subject to the GDPR. However, how can the provisions of the GDPR, especially the ones with an administrative nature,[438] be enforced against said operator in case of non-compliance? While it is true that unenforceable laws can, in certain cases, have a value of their own, such assertions of legislative jurisdiction with no possibility of enforcement should be practiced with care, and it can be concluded that the GDPR appears to take unenforceable assertions a step too far. Therefore, although it might not be possible to conclude whether a certain assertion of jurisdiction is completely illegitimate under public international law, some of these assertions can still be considered questionable and criticised – by resorting to such kinds of assertions of jurisdiction, the EU embarks on a dangerous journey that can, at worst, even result in loss of respect for the EU data protection regime abroad.[439]

However, while it may seem at first that the EU aims to globally regulate almost everything related to processing of personal data, this is also not the case, as it was cautiously implied in the recent CJEU case C-507/17 – *Google.* While the Court did not exclude the possibility of global enforcement of the right to be forgotten, it highlighted that the right to the protection of personal data is not absolute and that it is important to balance between it and other fundamental rights.[440] This approach can be seen as a voice of reason that is possibly even slightly toning down some of the most broad assertions of jurisdiction made in the GDPR.[441]

Although the Court did consider the balancing between different fundamental rights, it appears that the Court did not perform a proper balancing test between the interests of

---

[437] Regardless of the fact that from a European perspective, the GDPR’s extraterritorial effects have a strong foundation in the primary EU law and the fundamental rights of the EU, constituting the EU’s strong interest to regulate data protection extraterritorially.

[438] For instance, the “administrative” provisions identified by Svantesson, such as the requirements concerning the data protection officers and data protection by design and by default (Svantesson 2013a, p. 281).

[439] See section 2.4.2 above.

[440] Such a trend is also apparent in other recent CJEU case law concerning the right to data protection, see, e.g., C-136/17 – *GC and Others*, para 57–59, 66; C-496/17 – *Deutsche Post*, para 64–68; and C-345/17 – *Buivids,* para 64–69. See also the recital 4 of the GDPR.

[441] However, the possibility of derogation from the judgment presented in para 72 makes it somewhat unclear, what the actual impact of the judgment will be.

different regulators, and assess whether the interest of the EU does transcend the interests of non-EU states.[442] As noted above, performing such a balancing test would be essential in order to establish whether an assertion of jurisdiction outside the EU can be considered fair and justified from an international perspective. On a theoretical level, a proper balancing test might call for an introduction of "layered" data protection requirements that would increase proportionally with the level of connection between the EU and the data processing activity in question and with the EU's interest to regulate such activity. However, as such approach would require a complete legislative reform and would most likely create more uncertainty and questions than it can resolve, such approach cannot be considered viable, at least in the near future.

Regardless of the issues associated with the "layered" approach, the performance of such a balancing test could also guide the EU towards the increased use of such kinds of effects abroad, which do not excessively – or at all – encroach on the prerogatives of sovereign non-EU states. Above, such type of influence on the data processing activities of operators abroad was called "friendly" extraterritoriality. At the core of "friendly" extraterritoriality are, firstly, the domestically enforceable mechanisms of the GDPR, such as applicability to an establishment in the EU and the regulation of international data transfers. Secondly, "friendly" extraterritoriality is composed of the mechanisms that do not depend on enforcement at all, such as the bilateral and multilateral cooperation and the Brussels effect. Essentially, the legislative assertions of the European Union should, at least mostly and where appropriate, be supported by the possibility of enforcement, and the utilisation of such assertions should be maximised. However, should such types of assertions fail to ensure the sufficient protection of the fundamental rights of individuals within the EU, market blocking measures could be resorted to in cases where no other type of enforcement action is possible.

Returning to the CJEU judgment mentioned above, enforceability of an assertion of legislative jurisdiction is not everything, and the content of the actual enforcement action itself matters, too. While it may be possible for an authority within the EU to enforce, for instance, the performance of a data subject right globally under the penalty of a fine against an operator's establishment in the EU,[443] it does not necessarily mean that such

[442] See C-507/17 – *Google*, para 59, where the Court only acknowledged that "numerous third States do not recognise the right to de-referencing or have a different approach to that right."

[443] Such as it is for CNIL, if, in accordance with para 72 of C-507/17 – *Google*, it decides that a global enforcement is appropriate.

enforcement action should be taken. Again, a balancing of interests should be performed in order to assess whether such enforcement action would be questionable from the points of view of comity and sovereign equality.[444] For instance, a global right to be forgotten under EU law would be in an apparent contradiction with the First Amendment to the US Constitution, and the enforcement of such a right would be a significant invasion into the domestic affairs of a non-EU state.

From the point of view of comity, the CJEU judgment in C-507/17 – *Google* is a step in the right direction. While the balancing carried out in the judgment can be considered insufficient, it demonstrated that the EU acknowledges that the right to data protection is not unrestricted, and that there are territorial differences in how fundamental rights are balanced outside the EU. However, only time will tell what the actual influence of the judgment will be – currently, it has been left to CNIL's discretion to decide whether it will pursue global de-referencing of internet search results.

[444] See Kuner 2015a, p. 245.